#2

TENT APPLICATION

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the Application of

Masaki KYOJIMA, Kil-ho SHIN

Application No.: New U.S. Patent Application

Filed: October 3, 2000 Docket No.: 107500

For: LICENSE-ISSUING SYSTEM AND METHOD

CLAIM FOR PRIORITY

Director of the U.S. Patent and Trademark Office
Washington, D.C. 20231

Sir:

The benefit of the filing date of the following prior foreign application filed in the following foreign country is hereby requested for the above-identified patent application and the priority provided in 35 U.S.C. §119 is hereby claimed:

Japanese Patent Application No. 2000-024525 filed February 2, 2000

In support of this claim, a certified copy of said original foreign application:

__X__ is filed herewith.

_____ was filed on _____ in Parent Application No. _____ filed _____.

It is requested that the file of this application be marked to indicate that the requirements of 35 U.S.C. §119 have been fulfilled and that the Patent and Trademark Office kindly acknowledge receipt of this document.

Respectfully submitted,

James A. Oliff
Registration No. 27,075

Thomas J. Pardini
Registration No. 30,411

JAO:TJP/cmm
Date: October 3, 2000

OLIFF & BERRIDGE, PLC
P.O. Box 19928
Alexandria, Virginia 22320
Telephone: (703) 836-6400

DEPOSIT ACCOUNT USE AUTHORIZATION
Please grant any extension necessary for entry;
Charge any fee due to our Deposit Account No. 15-0461

日本国特許庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されてる事項と同一であることを証明する。
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２０００年　２月　１日

出願番号
Application Number: 特願２０００－０２４５２５

出願人
Applicant (s): 富士ゼロックス株式会社

２０００年　７月２１日

特許庁長官
Commissioner,
Patent Office 及川耕造

出証番号　出証特２０００－３０５６４２２

【書類名】　特許願
【整理番号】　FE00-00025
【提出日】　平成12年 2月 1日
【あて先】　特許庁長官殿
【国際特許分類】　G06F 17/00
【発明の名称】　利用許可証発行装置および方法
【請求項の数】　31
【発明者】
【住所又は居所】　神奈川県足柄上郡中井町境４３０　グリーンテクなかい
富士ゼロックス株式会社内
【氏名】　京嶋　仁樹
【発明者】
【住所又は居所】　神奈川県足柄上郡中井町境４３０　グリーンテクなかい
富士ゼロックス株式会社内
【氏名】　申　吉浩
【特許出願人】
【識別番号】　000005496
【氏名又は名称】　富士ゼロックス株式会社
【電話番号】　0462-38-8516
【代理人】
【識別番号】　100086531
【弁理士】
【氏名又は名称】　澤田　俊夫
【電話番号】　03-5541-7577
【手数料の表示】
【予納台帳番号】　038818
【納付金額】　21,000円
【提出物件の目録】
【物件名】　明細書　1

【物件名】　　図面　1

【物件名】　　要約書　1

【プルーフの要否】　　要

【書類名】　明細書

【発明の名称】　利用許可証発行装置および方法

【特許請求の範囲】

【請求項１】　デジタルコンテンツの利用が特定のユーザに対して許可されていることを証明する電子的な利用許可証を発行する方法であって、

利用許可証の正当性を検証するために必要な検証用情報を作成するステップと、

検証用情報を特定するための情報を入力するステップと、

入力された検証用情報を特定するための情報によって特定される検証用情報で検証可能な利用許可証を作成するステップと、

作成された利用許可証を出力するステップと

を備えていることを特徴とする利用許可証発行方法。

【請求項２】　デジタルコンテンツの利用が特定のユーザに対して許可されていることを証明する電子的な利用許可証を発行するコンピュータシステムであって、

利用許可証の正当性を検証するために必要な検証用情報を作成する検証用情報作成手段と、

上記検証用情報作成手段で作成された検証用情報を出力する検証用情報出力手段と、

検証用情報を特定するための情報が入力され、該入力によって特定される検証用情報で検証可能な利用許可証を作成する利用許可証作成手段と、

上記利用許可証作成手段で作成された利用許可証を出力する利用許可証出力手段と

を備えることを特徴とする利用許可証発行システム。

【請求項３】　デジタルコンテンツの利用を限定するための条件である利用条件を作成する利用条件作成手段を備え、

上記利用許可証作成手段が作成した利用許可証に、上記利用条件作成手段が作成した利用条件が含まれていることを特徴とする

請求項２記載の利用許可証発行システム。

【請求項４】　利用許可証作成手段が、

検証用情報を特定するための情報とともに、利用許可証発行の仲介者を特定するための情報と、該特定される検証用情報に対応する利用許可証の発行の仲介が該特定される仲介者に許諾されていることを証明する利用許可証仲介許諾証が入力され、

利用許可証仲介許諾証によって該仲介者に該検証用情報に対応する利用許可証の発行の仲介が許諾されているかを確認し、許諾されている場合にのみ利用許可証を作成することを特徴とする

請求項２記載の利用許可証発行システム。

【請求項５】　利用許可証の発行履歴を記憶する利用許可証発行履歴記憶部と、

デジタルコンテンツの提供者を特定するための情報の入力を受け、利用許可証発行履歴記憶部に記憶されている発行履歴から、該提供者が提供するデジタルコンテンツに関する利用許可証の発行履歴である利用許可証提供者用発行履歴を抽出する利用許可証提供者用発行履歴作成部と、

前記利用許可証提供者用発行履歴作成部で作成された利用許可証提供者用発行履歴を出力する利用許可証提供者用発行履歴出力部とをさらに備えることを特徴とする

請求項２記載の利用許可証発行システム。

【請求項６】　さらに、利用許可証の発行の依頼を受理する利用許可証発行依頼受理手段を備え、

上記利用許可証発行依頼受理手段が利用許可証発行依頼を受理した場合に、利用許可証作成手段で利用許可証を作成し、

利用許可証の発行履歴を記憶する利用許可証発行履歴記憶部と、

利用許可証発行の依頼者を特定するための情報の入力を受け、利用許可証発行履歴記憶部に記憶されている発行履歴から、該依頼者から依頼された利用許可証の発行履歴である利用許可証依頼者用発行履歴を抽出する利用許可証依頼者用発行履歴作成部と、

前記利用許可証依頼者用発行履歴作成部で作成された利用許可証依頼者用発行

履歴を出力する利用許可証依頼者用発行履歴出力部とをさらに備えることを特徴とする

請求項２記載の利用許可証発行システム。

【請求項７】　検証用情報の発行履歴を記憶する検証用情報発行履歴記憶部と、

検証用情報の被発行者を特定するための情報の入力をうけ、検証用情報発行履歴記憶部に記憶されている発行履歴から、該被発行者に対して発行された検証用情報に関する検証用情報の発行履歴である検証用情報発行被発行者用履歴を抽出する検証用情報発行履歴作成部と、

前記検証用情報発行履歴作成部で作成された検証用情報発行被発行者用履歴を出力する検証用情報発行履歴出力部とをさらに備えることを特徴とする

請求項２記載の利用許可証発行システム。

【請求項８】　さらに、公開鍵暗号ペアを作成する公開鍵暗号ペア作成手段と、

上記公開鍵暗号ペア作成手段で作成された公開鍵ペアのうちの秘密鍵を保持する秘密鍵保持手段とを備え、

検証用情報が上記公開鍵暗号ペア作成手段で作成された公開鍵であり、

利用許可証が秘密鍵保持手段に保持されている秘密鍵を使用して作成されることを特徴とする

請求項２記載の利用許可証発行システム。

【請求項９】　デジタルコンテンツの利用が特定のユーザに対して許可されていることを証明する電子的な利用許可証の依頼を仲介する方法であって、

特定のデジタルコンテンツの利用が許諾されていることを証する利用許可証の発行の依頼である第１の利用許可証依頼を受領するステップと、

受領した第１の利用許可証依頼で依頼されている利用許可証の発行を依頼する第２の利用許可証依頼を作成するステップと、

作成された第２の利用許可証依頼を出力するステップと

を有することを特徴とする利用許可証仲介方法。

【請求項１０】　デジタルコンテンツの利用が特定のユーザに対して許可さ

れていることを証明する電子的な利用許可証の依頼を仲介するコンピュータシステムであって、

特定のデジタルコンテンツの利用が許諾されていることを証する利用許可証の発行の依頼である第１の利用許可証依頼を受領する利用許可証依頼受領手段と、

受領した第１の利用許可証依頼で依頼されている利用許可証の発行を依頼する第２の利用許可証依頼を作成する利用許可証依頼作成手段と、

上記利用許可証依頼作成手段で生成された第２の利用許可証依頼を出力する利用許可証依頼出力手段と

を有することを特徴とする利用許可証仲介システム。

【請求項１１】　特定の利用許可証の正当性を検証するために必要な検証用情報が特定のデジタルコンテンツに対応づけられており、

第１および第２の利用許可証依頼に、該依頼が利用許可証を依頼するデジタルコンテンツを特定するために検証用情報を特定するための情報が含まれる

ことを特徴とする請求項１０記載の利用許可証仲介システム。

【請求項１２】　依頼する利用許可証がデジタルコンテンツの利用を限定するための条件である利用条件を含むものであり、

依頼する利用許可証に含まれるべき利用条件を作成する利用条件作成手段を備え、

利用許可証依頼作成手段が作成した第２の利用許可証依頼に、上記利用条件作成手段が作成した利用条件が含まれることを特徴とする

請求項１０記載の利用許可証仲介システム。

【請求項１３】　自らが特定のデジタルコンテンツに対する利用許可証の発行の仲介を許諾されていることを証明する利用許可証仲介許諾証を保持する利用許可証仲介許諾証記憶手段を備え、

利用許可証依頼出力手段が作成する利用許可証依頼に、利用の対象となるデジタルコンテンツに対するものであり、かつ、利用許可証仲介許諾証記憶手段に保持されている利用許可証仲介許諾証を添付することを特徴とする

請求項１０記載の利用許可証仲介システム。

【請求項１４】　さらに、第１の利用許可証依頼の依頼者に利用許可証発行

料金の課金を行う課金手段を備え、

第１の利用許可証を受領した時に、上記課金手段によって所定の利用許可証発行料金を該依頼者に対して課金することを特徴とする

請求項１０記載の利用許可証仲介システム。

【請求項１５】　さらに、第１の利用許可証依頼の依頼者から利用許可証発行料金を徴収する決済手段を備え、

第１の利用許可証依頼を受領した時に、上記決済手段によって所定の利用許可証発行料金を該依頼者から徴収することを特徴とする

請求項１０記載の利用許可証仲介システム。

【請求項１６】　デジタルコンテンツの利用が特定のユーザに対して許可されていることを証明する電子的な利用許可証の依頼の仲介を許諾する方法であって、

デジタルコンテンツの利用許可証の依頼を仲介する仲介者を特定するための情報を入力するステップと、

該仲介者に仲介を許諾するデジタルコンテンツを特定するための情報を入力するステップと、

入力によって特定されたデジタルコンテンツに対する利用許可証の依頼の仲介が入力によって特定された仲介者に許諾されていることを証明する利用許可証仲介許諾証を作成するステップと、

作成された利用許可証仲介許諾証を出力するステップとを有することを特徴とする利用許可証仲介許諾方法。

【請求項１７】　デジタルコンテンツの利用が特定のユーザに対して許可されていることを証明する電子的な利用許可証の依頼の仲介を許諾するコンピュータシステムであって、

デジタルコンテンツの利用許可証の依頼を仲介する仲介者を特定するための情報と、該仲介者に仲介を許諾するデジタルコンテンツを特定するための情報とが入力され、入力によって特定されたデジタルコンテンツに対する利用許可証の依頼の仲介が入力によって特定された仲介者に許諾されていることを証明する利用許可証仲介許諾証を作成する利用許可証仲介許諾証作成手段と、

上記利用許可証仲介許諾証作成手段で作成された利用許可証仲介許諾証を出力する利用許可証仲介許諾証出力手段と

を有することを特徴とする利用許可証仲介許諾システム。

【請求項１８】　許諾証の受け手である仲介者が仲介することで発行される利用許可証に記載される利用を限定するための条件である利用条件の範囲を限定するための情報である利用条件限定情報を作成する利用条件限定情報作成手段を備え、

上記利用許可証仲介許諾証作成手段が作成した利用許可証仲介許諾に、上記利用条件限定情報作成手段が作成した利用条件限定情報が含まれていることを特徴とする

請求項１７記載の利用許可証仲介許諾システム。

【請求項１９】　許諾証の発行履歴を記憶する利用許可証仲介許諾証発行履歴記憶部と、

利用許可証の依頼の仲介者を特定するための情報の入力を受け、利用許可証仲介許諾証発行履歴記憶部に記録されている発行履歴から、該仲介者に対して発行された許諾証に関する履歴である利用許可証仲介許諾証発行仲介者用履歴を抽出する利用許可証仲介許諾証発行仲介者用履歴作成部と、

前記利用許可証仲介許諾証発行仲介者用履歴作成部で作成された利用許可証仲介許諾証発行仲介者用履歴を出力する利用許可証仲介許諾証発行仲介者用履歴出力部とをさらに備えることを特徴とする

請求項１７記載の利用許可証仲介許諾システム。

【請求項２０】　ユーザに一つ以上の機能を提供する方法であって、

すべてあるいは一部の機能の利用が特定のユーザに対して許可されていることを証明する電子的な利用許可証を検証するための検証用情報を記憶するステップと、

利用許可証を入力するステップと、

入力された利用許可証の正当性を記憶されている検証用情報を使用して検証するステップと、

入力された利用許可証が正しいと判断された場合にのみ、自己が保持する機能

のうち少なくとも一部を動作可能にするステップと

を含む事を特徴とする機能提供方法。

【請求項２１】　デジタルコンテンツを操作する方法であって、

デジタルコンテンツの操作が特定のユーザに対して許可されていることを証明する電子的な利用許可証を検証するための検証用情報を記憶するステップと、

利用許可証を入力するステップと、

入力された利用許可証の正当性を記憶されている検証用情報を使用して検証するステップと、

入力された利用許可証が正しいと判断された場合にのみ、デジタルコンテンツに対する操作のうちの少なくとも一部を動作可能にするステップと

を含む事を特徴とするデジタルコンテンツ操作方法。

【請求項２２】　暗号化されたデジタルコンテンツを復号する方法であって、

デジタルコンテンツの復号が特定のユーザに対して許可されていることを証明する電子的な利用許可証を検証するための検証用情報を記憶するステップと、

利用許可証を入力するステップと、

入力された利用許可証の正当性を記憶されている検証用情報を使用して検証するステップと、

入力された利用許可証が正しいと判断された場合にのみ、入力されたデジタルコンテンツを復号するステップと

を含む事を特徴とするデジタルコンテンツ復号方法。

【請求項２３】　圧縮されたデジタルコンテンツを伸長する方法であって、

デジタルコンテンツの伸長が特定のユーザに対して許可されていることを証明する電子的な利用許可証を検証するための検証用情報を記憶するステップと、

利用許可証を入力するステップと、

入力された利用許可証の正当性を記憶されている検証用情報を使用して検証するステップと、

入力された利用許可証が正しいと判断された場合にのみ、入力されたデジタルコンテンツを伸長するステップと

を含む事を特徴とするデジタルコンテンツ伸長方法。

【請求項２４】　ユーザに一つ以上の機能を提供する装置であって、

該装置のすべてあるいは一部の機能の利用が特定のユーザに対して許可されていることを証明する電子的な利用許可証を検証するための検証用情報を記憶する検証用情報記憶手段と、

利用許可証が入力され、その利用許可証の正当性を前記検証用情報記憶手段に記憶されている検証用情報を使用して検証する利用許可証検証手段とを有し、

該利用許可証検証手段で、入力された利用許可証が正しいと判断された場合にのみ、自己が保持する機能のうち少なくとも一部を動作可能にすること

を特徴とする装置。

【請求項２５】　デジタルコンテンツを操作する装置であって、

デジタルコンテンツの操作が特定のユーザに対して許可されていることを証明する電子的な利用許可証を検証するための検証用情報を記憶する検証用情報記憶手段と、

利用許可証が入力され、その利用許可証の正当性を前記検証用情報記憶手段に記憶されている検証用情報を使用して検証する利用許可証検証手段とを有し、

該利用許可証検証手段で、入力された利用許可証が正しいと判断された場合にのみ、デジタルコンテンツに対する操作のうちの少なくとも一部を動作可能にすること

を特徴とするデジタルコンテンツ操作装置。

【請求項２６】　該検証用情報がデジタルコンテンツに含まれており、

該検証用情報をデジタルコンテンツから取り出して、該検証用情報記憶手段に記憶する

ことを特徴とする請求項２５記載のデジタルコンテンツ操作装置。

【請求項２７】　暗号化されたデジタルコンテンツを復号する装置であって、

デジタルコンテンツの復号が特定のユーザに対して許可されていることを証明する電子的な利用許可証を検証するための検証用情報を記憶する検証用情報記憶手段と、

利用許可証が入力され、その利用許可証の正当性を前記検証用情報記憶手段に記憶されている検証用情報を使用して検証する利用許可証検証手段とを有し、

該利用許可証検証手段で、入力された利用許可証が正しいと判断された場合にのみ、入力されたデジタルコンテンツを復号すること

を特徴とするデジタルコンテンツ復号装置。

【請求項２８】　該検証用情報が暗号化されたデジタルコンテンツに含まれており、

該検証用情報を暗号化されたデジタルコンテンツから取り出して、該検証用情報記憶手段に記憶する

ことを特徴とする請求項２７記載のデジタルコンテンツ復号装置。

【請求項２９】　圧縮されたデジタルコンテンツを伸長する装置であって、

伸長の対象となる圧縮されたデジタルコンテンツを入力する手段と、

デジタルコンテンツの伸長が特定のユーザに対して許可されていることを証明する電子的な利用許可証を検証するための検証用情報を記憶する検証用情報記憶手段と、

利用許可証が入力され、その利用許可証の正当性を前記検証用情報記憶手段に記憶されている検証用情報を使用して検証する利用許可証検証手段とを有し、

該利用許可証検証手段で、入力された利用許可証が正しいと判断された場合にのみ、入力されたデジタルコンテンツを伸長すること

を特徴とするデジタルコンテンツ伸長装置。

【請求項３０】　該検証用情報が圧縮されたデジタルコンテンツに含まれており、

該検証用情報を圧縮されたデジタルコンテンツから取り出して、該検証用情報記憶手段に記憶する

ことを特徴とする請求項２９記載のデジタルコンテンツ伸長装置。

【請求項３１】　さらに、利用許可証を保持している携帯用記憶装置を接続する接続手段を備え、

利用許可証検証手段が、上記接続手段を通して接続された携帯用記憶装置に記憶されている利用許可証の正当性を検証することを特徴とする

請求項２４～３０のいずれかに記載の利用許可証検証装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、コンピュータシステムにおいてデジタルコンテンツの利用を許可する技術に関わり、特に、ユーザがデジタルコンテンツの利用を許可されていることを証する利用許可証の発行や、該利用許可証の正当性の検証に関する。

【０００２】

【従来の技術】

インターネットの急速な普及に伴い、画像、音声、映像といったデジタルデータあるいはソフトウエアといったデジタルコンテンツをインターネット経由で提供し、対価を得るというビジネスが広がりつつある。デジタルコンテンツの提供者の立場にたてば、インターネットを利用すれば、デジタルコンテンツのパッケージングや流通のためのコストを省くことができるというメリットがあり、また、消費者からみれば、家庭にいながらでもデジタルコンテンツを入手できるというメリットがある。インターネット経由のデジタルコンテンツの提供は、今後、デジタルコンテンツを対象としたビジネスの主流になっていくことは疑いない。

【０００３】

現在のデジタルコンテンツの販売において最も問題なのは、デジタルコンテンツの利用者から正しく対価を徴収するのが困難なことである。最近では、電子的な決済手段が整い始め、金銭の授受自体は安全に行えるようになりつつある。したがって、デジタルコンテンツの利用者に正しく対価を支払う意志がある限りは、問題が起こりにくくなってきた。しかし、何の痕跡もなく複製が可能であるというデジタルコンテンツの特徴により、対価を支払う意志のないものがコンテンツを複製し、使用することは非常に容易である。

【０００４】

この問題に関して、現在もっとも多く取られている方法が、サイトのアクセスコントロールである。

【０００５】

この方法では、消費者は、デジタルコンテンツをインターネット上にあるサイトからダウンロードする。そのサイトにはアクセスコントロールがかけてあり、対価を支払った消費者のみがデジタルコンテンツをダウンロードすることが可能である。サイトにアクセスした消費者からは対価が徴収できるものの、ダウンロードした後のデジタルコンテンツは複製が可能であり、その複製の利用者からは対価を得ることができないことが問題である。しかし、少なくともデジタルコンテンツをダウンロードした消費者からは対価が得られること、また、仕組みが簡便で導入しやすいことから、この方法を利用している業者は多い。

【０００６】

複製したデジタルコンテンツの利用者からかも対価を徴収するために考案された手段が、ソフトウエアキーと呼ばれる利用許可証を利用した方法である。主にソフトウエアの販売に利用される方法であり、シェアウエアの代金回収に用いられることが多い。

【０００７】

この方法では、デジタルコンテンツの提供者は、自己が提供するデジタルコンテンツに対して有効なソフトウエアキーと呼ばれるデジタルデータの集合と、そのソフトウエアキーの有効性を検証する方法とを決定する。デジタルコンテンツにはソフトウエアキーの検証方法が実装され、有効なソフトウエアキーが提示されたときにのみ、自己の利用を許すように作成される。ソフトウエアキーは、デジタルコンテンツの対価を払った消費者にのみ送付されるので、デジタルコンテンツを利用できるのはデジタルコンテンツの対価を支払った消費者のみとなる。逆にいえば、デジタルコンテンツを使用したい消費者は、デジタルコンテンツの提供者から必ずソフトウエアキーを購入しなければならない。

【０００８】

【発明が解決しようとする課題】

デジタルコンテンツの提供者が有効なソフトウエアキーの集合とそのソフトウエアキーの有効性を検証する方法とを決定する仕組みでは、ソフトウエアキーに関する開発コストや、ソフトウエアキーを販売・発行する運営コストをデジタルコンテンツの提供者が負わなければならない。ソフトウエアキーは、デジタルコ

ンテンツに対する消費者の利用権を証する利用許可証ともいえるデジタルデータであり、漏洩、偽造、複製といったセキュリティ上の様々な問題に対する耐性が必要となる。このような仕組みの開発や運営はコストの上昇をもたらし、デジタルコンテンツの提供者がこのソフトウエアキーを利用したデジタルコンテンツのオンライン販売に乗り出す際の重大な障壁になるとともに、販売価格の上昇という不利益を消費者にもたらす。

【０００９】

【課題を解決するための手段】

本発明では、販売される特定のデジタルコンテンツあるいはデジタルコンテンツ提供者、あるいは、デジタルコンテンツ販売業者とは独立の利用許可証の発行を担うサーバ（以降、利用許可証発行センタあるいは単にセンタとよぶ）をインターネット上に構築することで、上記の課題を解決する。利用許可証の作成や維持に関わる部分は利用許可証発行センタがすべて引き受け、デジタルコンテンツの販売を行う業者は利用許可証に関わる部分の多くを利用許可証発行センタにアウトソーシングすることができる。多くの業者が共通の利用許可証発行センタを使用することが可能なので、業者一つあたりの利用許可証発行センタの開発・運営コストは業者が独自のシステムを構築するのにくらべて低く押さえることができる。

【００１０】

本発明では、デジタルコンテンツ販売業者は、消費者から受けたデジタルコンテンツの購入依頼に対して利用許可証を発行するが、その利用許可証は利用許可証発行センタで生成される。該業者は、消費者からの購入依頼を受け付けるサーバをインターネット上に構築するが、許可証を生成する部分は該サーバ中には存在せず、利用許可証発行センタがその役割を担う。

【００１１】

デジタルコンテンツの利用時には、消費者は利用許可証を提示し、利用許可証の正当性が確認されたときにのみコンテンツの利用が可能になるが、この検証は検証用情報と呼ばれるデジタルデータを使用して行われる。検証用情報は複数の利用許可証との間に所定の関係を満たすように生成されており、検証用情報と利

用許可証がその関係を満たすかどうかで利用許可証の正当性が判定される。特定のデジタルコンテンツと特定の検証用情報をバインドさせておけば、その検証用情報と所定の関係を満たす利用許可証を提示できるかどうかで、消費者がデジタルコンテンツを購入したかどうかが判定できる。

【００１２】

検証用情報は、センタで生成され出力される。どの業者が販売した利用許可証であっても対応する検証用情報を入手していればその正当性を検証することが可能である。

【００１３】

この特徴は、デジタルコンテンツの販売ビジネスに乗り出す業者が払うべきコストを更に下げる効果を持つ。本発明では、デジタルコンテンツの提供者と、それらの販売業者は互いに独立に存立できる。デジタルコンテンツの提供者は、自分が提供するデジタルコンテンツの販売を多くの販売業者に委託し、自己はデジタルコンテンツの提供に専念することができる。また、販売業者は、自らが提供するデジタルコンテンツをまったく持たなくても、様々な提供者が提供する多くのデジタルコンテンツを販売する事が可能である。

【００１４】

請求項１または２に記載の発明は利用許可証発行センタに関するものである。

【００１５】

請求項１に記載の発明は、デジタルコンテンツの利用が特定のユーザに対して許可されていることを証明する電子的な利用許可証を発行する方法であって、利用許可証の正当性を検証するために必要な検証用情報を作成するステップと、検証用情報を特定するための情報が入力するステップと、入力された検証用情報を特定するための情報によって特定される検証用情報で検証可能な利用許可証を作成するステップと、作成された利用許可証を出力するステップとを備える。

【００１６】

また、請求項２に記載の発明は、デジタルコンテンツの利用が特定のユーザに対して許可されていることを証明する電子的な利用許可証を発行するコンピュータシステムであって、利用許可証の正当性を検証するために必要な検証用情報を

作成する検証用情報作成手段と、上記検証用情報作成手段で作成された検証用情報を出力する検証用情報出力手段と、検証用情報を特定するための情報が入力され、該入力によって特定される検証用情報で検証可能な利用許可証を作成する利用許可証作成手段と、上記利用許可証作成手段で作成された利用許可証を出力する利用許可証出力手段とを備える。

【００１７】

請求項１または２に記載の発明によるセンタは、利用許可証を発行するだけでなく、利用許可証を検証するための検証用情報も出力する。この検証用情報はデジタルコンテンツの利用の際に消費者から提示される利用許可証の正当性を検証する際に使用される。特定の検証用情報によって検証可能な利用許可証の集合は限定されるので、特定のデジタルコンテンツの検証用情報を割り当てることで、デジタルコンテンツ毎の利用許可証の発行が可能である。しかし、どの検証用情報（あるいはそれに対応する利用許可証の集合）がどのデジタルコンテンツに対応するかに関してセンタは関与する必要はない。デジタルコンテンツと検証用情報との連結はデジタルコンテンツの提供者が自由に決定することができる。このことが、利用許可証発行センタを、特定のデジタルコンテンツに関与しない利用許可証の発行にのみ特化したインフラストラクチャたらしめることを可能にする。

【００１８】

請求項９または１０に記載の発明は、デジタルコンテンツの販売を行うサーバに関するものである。

【００１９】

請求項９に記載の発明は、デジタルコンテンツの利用が特定のユーザに対して許可されていることを証明する電子的な利用許可証の依頼を仲介する方法であって、特定のデジタルコンテンツの利用が許諾されていることを証する利用許可証の発行の依頼である第１の利用許可証依頼を受領するステップと、受領した第１の利用許可証依頼で依頼されている利用許可証の発行を依頼する第２の利用許可証依頼を作成するステップと、作成された第２の利用許可証依頼を出力するステップとを有することを特徴とする。

【００２０】

また、請求項１０に記載の発明は、デジタルコンテンツの利用が特定のユーザに対して許可されていることを証明する電子的な利用許可証の依頼を仲介するコンピュータシステムであって、特定のデジタルコンテンツの利用が許諾されていることを証する利用許可証の発行の依頼である第１の利用許可証依頼を受領する利用許可証依頼受領手段と、受領した第１の利用許可証依頼で依頼されている利用許可証の発行を依頼する第２の利用許可証依頼を作成する利用許可証依頼作成手段と、上記利用許可証依頼作成手段で生成された第２の利用許可証依頼を出力する利用許可証依頼出力手段とを有することを特徴とする。

【００２１】

請求項９または１０に記載の発明を適用した、デジタルコンテンツの販売を行うサーバは、インターネットに接続している消費者あるいは他の販売業者からの利用許可証発行の依頼を受けつける。しかし、受け付けた依頼に対する利用許可証を作成するのはこのサーバではない。利用許可証の発行は利用許可証発行センタのみが行い、デジタルコンテンツの販売を行うサーバは、利用許可証に対する依頼の仲介のみを行う。該サーバが行うのは、単に依頼の仲介のみであり、利用許可証の改竄、偽造、複製といった攻撃に対する配慮はセンタが行うので、本実施例に基づいたデジタルコンテンツの販売を行うサーバの構築費用や運営コストは低く押さえられる。

【００２２】

請求項１６または１７に記載の発明は、デジタルコンテンツの提供者に関するものである。

【００２３】

デジタルコンテンツの提供者と販売業者が独立に存立した場合、該提供者にとっては、自己が提供するデジタルコンテンツをより多くの販売業者に販売をしてもらうほうが、基本的には有利である。しかし、信頼できない販売業者に自己のデジタルコンテンツを扱われることは、後のトラブルを招く恐れが高く許容できない。したがって、デジタルコンテンツの提供者が、自己のデジタルコンテンツを扱える販売業者を限定できる手段が必要になる。

【００２４】

請求項１６に記載の発明は、デジタルコンテンツの利用が特定のユーザに対して許可されていることを証明する電子的な利用許可証の依頼の仲介を許諾する方法であって、デジタルコンテンツの利用許可証の依頼を仲介する仲介者を特定するための情報を入力するステップと、該仲介者に仲介を許諾するデジタルコンテンツを特定するための情報を入力するステップと、入力によって特定されたデジタルコンテンツに対する利用許可証の依頼の仲介が入力によって特定された仲介者に許諾されていることを証明する利用許可証仲介許諾証を作成するステップと、作成された利用許可証仲介許諾証を出力するステップとを有することを特徴とする。

【００２５】

また、請求項１７に記載の発明は、デジタルコンテンツの利用が特定のユーザに対して許可されていることを証明する電子的な利用許可証の依頼の仲介を許諾するコンピュータシステムであって、デジタルコンテンツの利用許可証の依頼を仲介する仲介者を特定するための情報と、該仲介者に仲介を許諾するデジタルコンテンツを特定するための情報とが入力され、入力によって特定されたデジタルコンテンツに対する利用許可証の依頼の仲介が入力によって特定された仲介者に許諾されていることを証明する利用許可証仲介許諾証を作成する利用許可証仲介許諾証作成手段と、上記利用許可証仲介許諾証作成手段で作成された利用許可証仲介許諾証を出力する利用許可証仲介許諾証出力手段とを有することを特徴とする。

【００２６】

請求項１６または１７に記載の発明によれば、デジタルコンテンツの提供者は、自己が提供するデジタルコンテンツの販売を許す販売業者に対して利用許可証仲介許諾証を発行する。この利用許可証仲介許諾証は、販売業者が利用許可証の発行をセンタに依頼する場合にセンタに対して提示される。センタは提示された利用許可証仲介許諾証により、該販売業者が利用許可証の発行を依頼したデジタルコンテンツに対する仲介を許諾されているかどうかを検査することができる。

【００２７】

請求項２０または２４に記載の発明は、消費者に提供されるデジタルコンテンツ自体に関するものであり、とくに、消費者が自己を利用可能な利用許可証を所持しているかどうかを検査する機能をもつものである。

【００２８】

請求項２０に記載の発明は、ユーザに一つ以上の機能を提供する方法であって、すべてあるいは一部の機能の利用が特定のユーザに対して許可されていることを証明する電子的な利用許可証を検証するための検証用情報を記憶するステップと、利用許可証を入力するステップと、入力された利用許可証の正当性を記憶されている検証用情報を使用して検証するステップと、入力された利用許可証が正しいと判断された場合にのみ、自己が保持する機能のうち少なくとも一部を動作可能にするステップとを備える。

【００２９】

請求項２４に記載の発明は、ユーザに一つ以上の機能を提供する装置であって、該装置のすべてあるいは一部の機能の利用が特定のユーザに対して許可されていることを証明する電子的な利用許可証を検証するための検証用情報を記憶する検証用情報記憶手段と、利用許可証が入力され、その利用許可証の正当性を前記検証用情報記憶手段に記憶されている検証用情報を使用して検証する利用許可証検証手段とを有し、該利用許可証検証手段で、入力された利用許可証が正しいと判断された場合にのみ、自己が保持する機能のうち少なくとも一部を動作可能にすることを特徴とする。

【００３０】

請求項２１または２５に記載の発明は、消費者に提供されるデジタルコンテンツを操作する装置あるいはソフトウエアに関するものであり、とくに、消費者がデジタルコンテンツを操作可能な利用許可証を所持しているかどうかを検査する機能をもつものである。

【００３１】

請求項２１に記載の発明は、デジタルコンテンツを操作する方法であって、デジタルコンテンツの操作が特定のユーザに対して許可されていることを証明する電子的な利用許可証を検証するための検証用情報を記憶するステップと、利用許

可証を入力するステップと、入力された利用許可証の正当性を記憶されている検証用情報を使用して検証するステップと、入力された利用許可証が正しいと判断された場合にのみ、デジタルコンテンツに対する操作のうちの少なくとも一部を動作可能にするステップとを備える。

【００３２】

請求項２５に記載の発明は、デジタルコンテンツを操作する装置であって、デジタルコンテンツの操作が特定のユーザに対して許可されていることを証明する電子的な利用許可証を検証するための検証用情報を記憶する検証用情報記憶手段と、利用許可証が入力され、その利用許可証の正当性を前記検証用情報記憶手段に記憶されている検証用情報を使用して検証する利用許可証検証手段とを有し、該利用許可証検証手段で、入力された利用許可証が正しいと判断された場合にのみ、デジタルコンテンツに対する操作のうちの少なくとも一部を動作可能にすることを特徴とする。

【００３３】

請求項２２または２７に記載の発明は、消費者に提供される暗号化されたデジタルコンテンツを復号する装置あるいはソフトウエアに関するものであり、とくに、消費者がデジタルコンテンツを復号可能な利用許可証を所持しているかどうかを検査する機能をもつものである。

【００３４】

請求項２２に記載の発明は、暗号化されたデジタルコンテンツを復号する方法であって、デジタルコンテンツの復号が特定のユーザに対して許可されていることを証明する電子的な利用許可証を検証するための検証用情報を記憶するステップと、利用許可証を入力するステップと、入力された利用許可証の正当性を記憶されている検証用情報を使用して検証するステップと、入力された利用許可証が正しいと判断された場合にのみ、入力されたデジタルコンテンツを復号するステップとを備える。

【００３５】

請求項２７に記載の発明は、暗号化されたデジタルコンテンツを復号する装置であって、デジタルコンテンツの復号が特定のユーザに対して許可されているこ

とを証明する電子的な利用許可証を検証するための検証用情報を記憶する検証用情報記憶手段と、利用許可証が入力され、その利用許可証の正当性を前記検証用情報記憶手段に記憶されている検証用情報を使用して検証する利用許可証検証手段とを有し、該利用許可証検証手段で、入力された利用許可証が正しいと判断された場合にのみ、入力されたデジタルコンテンツを復号することを特徴とする。

【００３６】

請求項２３または２９に記載の発明は、消費者に提供される圧縮されたデジタルコンテンツを伸長する装置あるいはソフトウエアに関するものであり、とくに、消費者がデジタルコンテンツを伸長可能な利用許可証を所持しているかどうかを検査する機能をもつものである。

【００３７】

請求項２３に記載の発明は、圧縮されたデジタルコンテンツを伸長する方法であって、デジタルコンテンツの伸長が特定のユーザに対して許可されていることを証明する電子的な利用許可証を検証するための検証用情報を記憶するステップと、利用許可証を入力するステップと、入力された利用許可証の正当性を記憶されている検証用情報を使用して検証するステップと、入力された利用許可証が正しいと判断された場合にのみ、入力されたデジタルコンテンツを伸長するステップとを備える。

【００３８】

請求項２９に記載の発明は、圧縮されたデジタルコンテンツを伸長する装置であって、伸長の対象となる圧縮されたデジタルコンテンツを入力する手段と、デジタルコンテンツの伸長が特定のユーザに対して許可されていることを証明する電子的な利用許可証を検証するための検証用情報を記憶する検証用情報記憶手段と、利用許可証が入力され、その利用許可証の正当性を前記検証用情報記憶手段に記憶されている検証用情報を使用して検証する利用許可証検証手段とを有し、該利用許可証検証手段で、入力された利用許可証が正しいと判断された場合にのみ、入力されたデジタルコンテンツを伸長することを特徴とする。

【００３９】

なお、本発明はインターネットにおける利用に限定されるものではなく、広く

通信ネットワークに適用可能である。またネットワークにおける通信を利用せずに装置同志を用いて利用証明証を発行するようにしてもよいことはもちろんである。

【００４０】

【発明の実施の形態】

以下に、本発明の一実施形態について説明する。

【００４１】

図１は本発明を適用した実施例の構成図である。本実施例は、インターネットに接続した複数のコンピュータシステムからなり、これらが協調して動作することでデジタルコンテンツの販売を行う。

【００４２】

本実施例では、消費者はデジタルコンテンツの購入をインターネット経由で行い、購入が完了したことを証するデジタルデータである利用許可証を受け取る。

【００４３】

デジタルコンテンツは、利用許可証を持つ消費者のみが利用可能なような形態で消費者に対して提供される。利用者は、利用許可証を所持している場合にのみ、デジタルコンテンツを使用することが可能である。

【００４４】

［実施例を構成するコンピュータシステム群］

本実施例を構成するコンピュータシステムは以下の４つの種類に分類される。それぞれインターネット１０１に接続され、相互に通信を行う。

【００４５】

消費者端末：消費者がデジタルコンテンツの購入を行う際に使用するコンピュータシステム。図１の１０７にあたる。消費者が家庭で使用するコンピュータであってもよいし、コンビニエンスストア等に設置されている端末でもよい。インターネット１０１に接続されており、インターネット１０１経由で他のコンピュータシステムにアクセスすることができる。

【００４６】

リテーラ：消費者に対してデジタルコンテンツの販売を行うコンピュータシステ

ム。図１の１０３あるいは１０４にあたり、実際にはいくつ存在してもかまわない。インターネット１０１に接続されており、インターネット１０１経由で消費者からのアクセスを受け付ける。リテーラを運営しているのはデジタルコンテンツの販売をしている業者であるが、以降の本実施例の説明では、該コンピュータシステムと該業者を区別せず、ともにリテーラと呼ぶ事にする。

【００４７】

利用許可証発行センタ：利用許可証を生成し発行するコンピュータシステム。図１の１０２にあたる。インターネット１０１に接続されており、インターネット経由でリテーラからの利用許可証の依頼を受け付け、オンデマンドで利用許可証を作成し発行する。以降、センタといえば利用許可証発行センタを指す。

【００４８】

プロバイダ：デジタルコンテンツの提供者がリテーラ１０３あるいは１０４やセンタ１０２と情報の交換を行うためのコンピュータシステムであり、インターネット１０１に接続される。図１の１０５、１０６にあたり、実際にはいくつ存在してもかまわない。以降の本実施例の説明では、デジタルコンテンツの提供者と該提供者が使用するコンピュータシステムを区別せず、ともにプロバイダと呼ぶ事にする。

【００４９】

認証局（Ｃｅｒｔｉｆｉｃａｔｅ　Ａｕｔｈｏｒｉｔｙ）：消費者端末、リテーラ、センタ、プロバイダのあいだで交わされる各メッセージには、改竄検知と否認拒否のためにデジタル署名が施される。そのデジタル署名の検証鍵の正当性はＸ．５０９ベースの公開鍵証明証によって保証される。Ｃｅｒｔｉｆｉｃａｔｅ　Ａｕｔｈｏｒｉｔｙ　１０８はこの公開鍵証明証を作成し発行する機能を持つコンピュータシステムであり、インターネット１０１に接続されている。また、Ｃｅｒｔｉｆｉｃａｔｅ　Ａｕｔｈｏｒｉｔｙは、自己が発行した公開鍵証明証を保持しており、オンデマンドで要求者に送付する機能も持つ。以降、ＣＡといえばＣｅｒｔｉｆｉｃａｔｅ　Ａｕｔｈｏｒｉｔｙを指す。

【００５０】

［利用許可証と検証用公開鍵］

本実施例では、消費者がデジタルコンテンツを購入したことを証明するために利用許可証と呼ばれるデジタルデータが発行される。利用許可証の正当性は対応する検証用公開鍵によって検証される。検証用公開鍵の名前が示すように、本実施例では利用許可証と検証用公開鍵には公開鍵暗号技術が応用される。

【００５１】

より具体的には、検証用公開鍵は公開鍵暗号における公開鍵であり、利用許可証は該公開鍵に対応する秘密鍵をもとに作成された証明値を含むデータである。利用許可証が含む証明値を作成する際に使用した秘密鍵と、検証用公開鍵が対応するものであった場合にのみ、利用許可証が正当なものであることが確認でき、それ以外の場合で利用許可証が正当なものであると認められることはない。

【００５２】

本実施例でデジタルコンテンツを販売する場合には、販売される特定のデジタルコンテンツあるいは、デジタルコンテンツが消費者に提供する特定の機能とバインドされる検証用公開鍵が必要である。特定の検証用公開鍵と特定のデジタルコンテンツあるいはその機能をバインドさせることで、特定のデジタルコンテンツやその機能の利用のみを許可する利用許可証を実現することができる。

【００５３】

利用許可証と検証用公開鍵に公開鍵暗号技術を利用しているのは、検証用公開鍵を公開可能とするためである。検証用公開鍵が公開鍵であれば、それを公開しても利用許可証の安全性を損なうことがない。このことは、検証用公開鍵の送受信や管理を楽にするだけでなく、利用許可証の正当性を第三者が検証できるようになり、後のトラブルを防ぐことが可能になるという利点がある。

【００５４】

検証用公開鍵はプロバイダからの依頼によって、センタ１０２で作成され、検証用公開鍵情報と呼ばれるデータに含まれて依頼者に送付される。センタ１０２は、検証用公開鍵の発行の要求を受け取ると新しい公開鍵ペアを作成し、その公開鍵と秘密鍵を、公開鍵ペアを一意に識別するための情報である検証用公開鍵識別子とともに保持した後、その公開鍵と検証用公開鍵識別子を含む検証用公開鍵情報を依頼者に送付する。検証用公開鍵情報を受け取ったプロバイダを、その検

証用公開鍵情報あるいは該検証用公開鍵情報に含まれる検証用公開鍵のユーザと呼ぶ。

【００５５】

特定の検証用公開鍵と特定のデジタルコンテンツあるいはその機能のバインドに関してセンタ１０２は関知しない。そのバインドを決定するのは、検証用公開鍵の発行を受けたプロバイダであり、該プロバイダは、自分が決定した、特定のデジタルコンテンツやその機能と検証用公開鍵とのバインドの情報を保持しておかなければならない。

【００５６】

利用許可証は、該許可証に対応する検証用公開鍵とバインドされた特定のデジタルコンテンツあるいはその機能の利用を許可するデータである。消費者がデジタルコンテンツを利用するコンピュータシステムに保持され、デジタルコンテンツの利用時にその正当性が検証される。

【００５７】

利用許可証がデジタルデータであるので、利用と許可された以外の利用者が利用許可証のコピーを使って、デジタルコンテンツを利用する危険がある。これを防止するために、利用許可証は消費者秘密情報とよばれる情報無しには、その正当性を検証できないように構成されている。消費者秘密情報は、利用許可証が正当であると認められる範囲を限定するための情報であり、ある消費者秘密情報にあわせて作成された利用許可証は、別の消費者秘密情報と共に利用しても正当なものと認められることはない。

【００５８】

たとえば、消費者秘密情報がコンピュータシステムに記憶されているコンピュータシステム毎に異なる数値として実現されれば、特定のコンピュータでのみ有効な利用許可証を実現することができる。この場合、消費者は、自分がそこでデジタルコンテンツを使うであろうコンピュータシステムが持つ消費者秘密情報にあわせた利用許可証を取得する。以降、該消費者は、該コンピュータシステムの上でのみデジタルコンテンツの利用が可能になるが、同じ利用証明証を使って他のコンピュータシステム上でデジタルコンテンツを利用することはできない。

【００５９】

デジタルコンテンツの使用が特定のコンピュータシステムに限定されるのが不便な場合は、ＩＣカード等の携帯型記憶装置を利用する。この場合、消費者秘密情報は、携帯型記憶装置に記憶されている携帯型記憶装置毎に異なるように実現される。この場合、消費者は、自分が所持する携帯型記憶装置に含まれる消費者秘密情報にあわせた利用許可証を取得する。以降、消費者は、自己が所持している携帯型記憶装置と取得した利用許可証を共に使用する場合に限りデジタルコンテンツを利用することができるが、携帯型記憶装置がなしにはデジタルコンテンツを利用することはできない。リムーバブルディスクやＭＯ等の記憶メディアを携帯型記憶装置として利用してもよい。

【００６０】

消費者秘密情報は、消費者すらその値を参照することができないように記憶されたデータとして実現される。また、コンピュータシステムや携帯型記憶装置の各種特徴量をもとに値を計算するアルゴリズムのみが記憶されており、消費者秘密情報が参照されるたびにそのアルゴリズムによる計算がおこなわれ、その結果が消費者秘密情報として使用されるのでもよい。その他にも実現方法はありえるが、いかなる方法であっても消費者秘密情報の内容を知っているのは利用許可証の発行者である利用許可証発行センタのみである。

【００６１】

各消費者秘密情報には、消費者識別子と呼ばれる識別子が割り当てられている。各消費者秘密情報がセンタ以外のエンティティにとって秘密のデータであるのと異なり、消費者識別子は誰でも参照できるデータである。消費者識別子は、消費者が利用許可証を依頼する際に、どの消費者秘密情報にあわせた利用許可証を要求しているのかを特定するために使用される。

【００６２】

特に本実施例では、消費者識別子は個々の消費者を特定するのにも使用される。同じ消費者が使っている複数のコンピュータであっても、それぞれが保持している消費者秘密情報が異なれば、別々の消費者識別子が割り当てられており、別々の消費者であると認識される。

【００６３】

検証用公開鍵情報のデータ構造は以下のようである。

【００６４】

【表１】

検証用公開鍵情報：：＝｛

発行者フィールド，
受領者フィールド，
発行日フィールド，
有効期間開始日時フィールド，
有効期間終了日時フィールド，
検証用公開鍵識別子フィールド，
公開鍵情報フィールド，
デジタル署名フィールド
｝

【００６５】

発行者フィールド：この検証用公開鍵情報の発行者であるセンタの識別子が記載される。

受領者フィールド：この検証用公開鍵情報の受領者であるプロバイダの識別子が記載される。

発行日フィールド：この検証用公開鍵情報の発行日が記載される。

有効期間開始日時フィールド：この検証用公開鍵情報の有効期間の開始日時が記載される。

有効期間終了日時フィールド：この検証用公開鍵情報の有効期間の終了日時が記載される。

検証用公開鍵識別子フィールド：センタがこの検証用公開鍵に割り当てた検証用公開鍵識別子が記載される。

公開鍵情報：利用許可証を検証する際に使用する検証用公開鍵の情報が記載される。使用する公開鍵暗号アルゴリズムの指定と、公開鍵の値を含む。

デジタル署名フィールド：発行者であるセンタによるこの検証用公開鍵情報全体

に対するデジタル署名が記載される。

【００６６】

利用許可証のデータ構造は以下のようである。

【００６７】

【表２】

利用許可証：：＝｛

発行者フィールド，

受領者フィールド，

発行日フィールド，

利用許可証識別子フィールド，

公開鍵識別子フィールド，

利用条件フィールド，

証明値フィールド，

デジタル署名フィールド

｝

【００６８】

発行者フィールド：この利用許可証の発行者であるセンタの識別子が記載される。

受領者フィールド：この利用許可証の受領者である消費者の識別子が記載される。

発行日フィールド：この利用許可証の発行日が記載される。

利用許可証識別子フィールド：センタがこの利用許可証に割り当てた識別子が記載される。

公開鍵識別子フィールド：この利用許可証に対応する検証用公開鍵に割り当てられた検証用公開鍵識別子が記載される。

利用条件フィールド：デジタルコンテンツの範囲を限定する条件である利用条件が記載される。

証明値フィールド：この利用許可証の公開鍵識別子フィールドに記載された識別子が割り当てられた検証用公開鍵に対応する秘密鍵をもとに作成された証明値が

記載される。

デジタル署名フィールド：発行者であるセンタによるこの利用許可証全体に対するデジタル署名が記載される。

【００６９】

利用条件フィールドに記載される。利用条件には、この利用許可証で有効となるデジタルコンテンツ利用の範囲を限定するための条件が記載される。

【００７０】

利用条件のデータ構造を以下に示す。

【００７１】

【表３】

利用条件：：＝｛

有効期間開始日時フィールド，

有効期間終了日時フィールド，

・・・

｝

【００７２】

有効期間開始日時フィールド：この利用許可証の有効期間の開始日時が記載される。この日時以前には、デジタルコンテンツの利用はできない。

有効期間終了日時フィールド：この利用許可証の有効期間の終了日時が記載される。この日時以降には、デジタルコンテンツの利用はできない。

【００７３】

利用条件に指定された各種条件は、利用許可証の検証時に該条件が満足されているかどうかが検査される。利用条件に指定された各種条件が満足されていなければ、利用許可証の正当性の検証に失敗する。

【００７４】

利用条件には、有効期間の開始日時または終了日時以外にも、利用許可証の用途に応じて種々のものが記載される。

【００７５】

例えば、デジタルコンテンツの利用回数が特定の回数以下に限定される場合に

は、その限定回数を利用条件に記載しておき、利用許可証の検査の際に該限定回数を超えていないかどうかを確認すればよい。

【００７６】

また、デジタルコンテンツの利用時にいくらかの料金を徴収する場合には、その金額を利用条件に記載しておき、利用許可証の検査の際に該料金をプリペイドの度数から引き落とす等の処理を実行すればよい。

【００７７】

あるいは、デジタルコンテンツが持つ機能のうちの特定の機能の利用のみを許す場合には、その機能を特定する情報を利用条件に記載しておき、利用許可証の検査の際にユーザが利用しようとする機能が利用条件に記載されたものであるかどうかを確認すればよい。

【００７８】

［証明値］

証明値は利用許可証に含まれるデータで、センタが作成した検証用公開鍵に対応する秘密鍵を元に作成されたデータであり、利用許可証が特定の検証用公開鍵とのみ対応する事を保証するためのものである。また、証明値の作成には、消費者秘密情報も使用され、特定のコンピュータシステム上での使用のみ許したり、あるいは、特定の携帯型記憶装置と組み合わせた場合にのみ使用を許したりといった制御も可能である。さらに、証明値の作成には、利用許可証に記載された利用条件も使用され、特定の利用条件を満足する場合にのみ利用可能である事も保証される。

【００７９】

証明値ｔは法数ｎ、検証用公開鍵ｅ、秘密鍵ｄ、消費者秘密情報ｕ、利用条件ｌから以下の式にしたがって作成される。

【００８０】

【数１】

$$t = d - f(n, e, u, l) \qquad (1)$$

ここで、関数ｆ（）は公開された一方向性関数である。たとえば、ＳＨＡ－１あるいはＭＤ５等の暗号学的一方向性ハッシュ関数が使用される。

【００８１】

式（１）でわかるように、証明値ｔは、法数ｎ、検証用公開鍵ｅ、消費者秘密情報ｕ、利用条件１とともに使用した場合にのみ秘密鍵ｄと同じ働きをする。どれ一つを差し替えても秘密鍵ｄと同じ働きをすることはない。

【００８２】

［利用許可証の検証とデジタルコンテンツの利用］

本実施例では、消費者がデジタルコンテンツを利用する際に、必要に応じて該デジタルコンテンツ全体、あるいはその一部の機能に対する利用許可証の正当性を検証し、デジタルコンテンツ全体あるいはその一部の機能の使用の利用を消費者が許可されているかどうかを検査し、許可されている場合にのみ利用を許す。

【００８３】

図３５は、本発明を適用したデジタルコンテンツであるアプリケーションソフトウエアの構成を示した図である。本ソフトウエアは、利用者からの命令により２つの機能を実行するが、どの機能も実行されるまえに、利用者が利用許可証を持っているかどうかが確認され、利用者が正しい利用許可証を所持する場合にのみ機能が実行される。それぞれの機能には異なる検証用公開鍵が割り当てられているので、それぞれ異なる利用証明証が必要である。

【００８４】

また、本ソフトウエアでは、消費者が消費者識別子と消費者秘密情報を含む携帯型記憶装置を所持しており、該消費者がデジタルコンテンツを使用するための利用許可証も該携帯型記憶装置に記憶されている。

【００８５】

本ソフトウエア３５０１は、入出力制御部３５０２、処理制御部３５０３、第１の機能の実行部３５０４、第２の機能の実行部３５０５、第１の利用許可証検査部３５０６、第２の利用許可証検査部３５０７、携帯型記憶装置制御部３５０８からなり、携帯型記憶装置制御部３５０８をとおして携帯型記憶装置３５１１と接続している。

【００８６】

それぞれの構成要素の役割を以下に示す。

【００８７】

入出力制御部３５０２：利用者からの入力あるいは、利用者への出力を制御する。

処理制御部３５０３：入出力制御部３５０２からの利用者の命令を受け取り、命令に応じて第１の機能の実行部３５０４、第２の機能の実行部３５０５を呼び出し、機能の実行の結果を受け取って、入出力制御部３５０２を介して利用者に出力する。

第１の機能の実行部３５０４：処理制御部３５０３からの呼び出しに応じて、第１の機能を実行し、結果を処理制御部３５０３に返す。実行の前に第１の利用許可証検査部３５０６を呼び出し、利用者が第１の機能に対応する正しい利用許可証を所持している事を確認する。

第２の機能の実行部３５０５：処理制御部３５０３からの呼び出しに応じて、第２の機能を実行し、結果を処理制御部３５０３に返す。実行の前に第２の利用許可証検査部３５０７を呼び出し、利用者が第２の機能に対応する正しい利用許可証を所持している事を確認する。

第１の利用許可証検査部３５０６：第１の機能の実行部３５０４からの呼び出しに応じて、利用者が第１の機能に対応する正しい利用許可証を所持しているかどうかを検査し、結果を第１の機能の実行部３５０４に返す。利用許可証の検査のために、携帯型記憶装置制御部３５０８を介して、携帯型記憶装置３５１１とデータの交換を行う。

第２の利用許可証検査部３５０７：第２の機能の実行部３５０５からの呼び出しに応じて、利用者が第２の機能に対応する正しい利用許可証を所持しているかどうかを検査し、結果を第２の機能の実行部３５０５に返す。利用許可証の検査のために、携帯型記憶装置制御部３５０８を介して、携帯型記憶装置３５１１とデータの交換を行う。

携帯型記憶装置制御部３５０８：携帯型記憶装置３５１１とのデータ交換を制御する。

【００８８】

図２８は、図３５に示したソフトウエアの第１の利用許可証検査部３５０６と

、該ソフトウエアに接続している携帯型記憶装置３５１１の内部構成を示したものである。第１の利用許可証検証部３５０６は、チャレンジと呼ぶ乱数値を携帯型記憶装置３５１１に送付し、携帯型記憶装置３５１１は受け取ったチャレンジと保持している利用許可証からレスポンスと呼ぶ値を計算して出力し、利用許可証検査部３５０６がレスポンスの正しさを検査する事で、携帯型記憶装置３５１１に保持されている利用許可証の正当性を検証する。

【００８９】

第１の利用許可証検査部３５０６は、条件判定対象情報生成部２８０１、チャレンジ生成部２８０２、公開鍵情報記憶部２８０３、レスポンス検査部２８０４から構成される。

【００９０】

利用許可証検査部３５０６の各部の役割を以下に示す。

【００９１】

条件判定対象情報生成部２８０１：利用許可証に記載されている利用条件が特定の条件を満たす場合にのみ第１の機能を実行する場合、その判断の対象となる情報を生成する。

チャレンジ生成部２８０２：携帯型記憶装置３５１１に送付するチャレンジを生成する。

公開鍵情報記憶部２８０３：第１の機能に割り当てられた検証用公開鍵の識別子と法数および公開鍵を保持する。

レスポンス検査部２８０４：携帯型記憶装置３５１１が作成したレスポンスの正しさを検査する。

【００９２】

また、携帯型記憶装置３５１１は入出力制御部２８１１、消費者秘密情報記憶部２８１２、レスポンス計算部２８１３、利用条件判定部２８１４、利用許可証記憶部２８１５から構成される。

【００９３】

携帯型記憶装置３５１１の各部の役割を以下に示す。

【００９４】

入出力制御部２８１１：ソフトウエア３５０１との間のデータの入出力を制御する。

消費者秘密情報記憶部２８１２：消費者秘密情報を保持する。

レスポンス計算部２８１３：第１の利用許可証検査部３５０６に送付するレスポンスを計算する。

利用条件判定部２８１４：利用許可証に記載されている利用条件が満たされているかどうかを判定する。

利用許可証記憶部２８１５：利用許可証が複数保持される。

【００９５】

図２９は、第１の機能に対する利用許可証の検査の際の第１の利用許可証検証部３５０６と携帯型記憶装置３５１１の動作を示すフローチャートである。図２９に従って利用許可証の検査の際の利用許可証検査部３５０６と携帯型記憶装置３５１１の動作を説明する。

【００９６】

利用許可証の検査の動作は第１の利用許可証検証部３５０６から始まる。

【００９７】

まず、チャンレンジ生成部２８０２でチャレンジＣが作成される（２９０１）。チャンレンジは検査を行うたびに異なる乱数値であり、チャンレンジ生成部２８０２は乱数生成機能を内包している。

【００９８】

チャレンジが生成された後、生成されたチャレンジＣ、公開鍵情報記憶部２８０３に保持されている検証用公開鍵の識別子ＩＤと法数ｎおよび公開鍵ｅ、条件判定対象情報生成部２８０１で生成された条件判定対象情報ｓが、携帯型記憶装置制御部３５０８を介して携帯型記憶装置３５１１に送付される（２９０２）。

【００９９】

Ｃ、ＩＤ、ｎ、ｅ、ｓを受け取った携帯型記憶装置３５１１は、まず利用許可証記憶部２８１５に保持されている利用許可証のうち検証用公開鍵識別子ＩＤに対応するものを選択する（２９０３）。この選択は、利用許可証記憶部２８１５に保持されている利用許可証のうち、その公開鍵識別子フィールドの値がＩＤと

等しいかどうかを調べる事で行われる。ここで該当する利用許可証が見つからなければ、エラーが入出力制御部２８１１を介して第１の利用許可証検査部３５０６に送付され（２９０８）、終了する。

【０１００】

該当する利用許可証が見つかった場合には、利用条件判定部２８１４で該利用許可証に含まれる利用条件１が満たされているかどうかが判定される（２９０４）。利用条件１に記載されている利用許可証の有効期間開始や終了のチェックのために、利用条件判定部２８１４は時計を内蔵している。また、第１の利用許可証検査部３５０６から条件指定ｓが入力されている場合、条件判定対象情報ｓが利用条件１を満たすかどうかもここで判定される。

【０１０１】

２９０４で、利用条件１が満たされていないと判断された場合、エラーが入出力制御部２８１１を介して第１の利用許可証検査部３５０６に送付され（２９０８）、終了する。

【０１０２】

２９０４で、利用条件１が満たされていると判断された場合、レスポンス計算部２８１３でレスポンスＲが計算され（２９０５）、入出力制御部２８１１を介して第１の利用許可証検査部３５０６に送付される（２９０６）。レスポンスＲは、入出力制御部２８１１を介して第１の利用許可証検査部３５０６から入力されたチャレンジＣ、法数ｎ、公開鍵ｅ、２９０３で選択された利用許可証に含まれる証明値ｔと利用条件１、消費者秘密情報記憶部２８１２に保持されている消費者秘密情報ｕから、以下の（２）式にしたがって計算される。

【０１０３】

【数２】

$$R = C^{t+f(n,e,u,l)} \quad \mathrm{mod} \quad n \qquad (2)$$

携帯型記憶装置制御部３５０８を介してレスポンスＲを受け取った第１の利用許可証検査部３５０６は、レスポンス検査部２８０４でレスポンスＲの正当性を検査する（２９０７）。検査にはレスポンスＲの他に、チャレンジ生成部２８０２が生成したチャレンジＣ、公開鍵情報記憶部２８０３が記憶している法数ｎ、

公開鍵ｅが使用される。（３）の式が成り立てば検証成功、そうでなければ失敗である。

【０１０４】

【数３】

$$C \equiv R^{e} \mod n \qquad (3)$$

（１）（２）（３）の式からわかるように、利用許可証の検査は、基本的には証明値ｔが秘密鍵ｄと同じ働きができるかどうかを判定する処理であり、法数や公開鍵、証明値、利用条件、消費者秘密情報の組み合わせが正しい時のみレスポンスの検証に成功する。検証用公開鍵が異なるデジタルコンテンツの利用許可証を流用したり、他人の利用許可証を利用したり、利用条件を改竄したりといった攻撃は困難である。

【０１０５】

前述したように、利用条件１には、利用許可証の有効期間以外に多くの条件が記載可能である。それらの条件のうち、条件判定の対象となる情報が携帯型記憶装置内にない場合は、その情報は携帯型記憶装置３５１１の外部から条件判定対象情報ｓとして供給される。たとえば、図３５に示したソフトウエアの第２の機能が実行された場合にのみ利用可能であると利用条件１に記載されている場合には、第２の機能が実行されたかどうかを示す情報が条件判定対象情報生成部２８０１で生成され、条件判定対象情報ｓとして携帯型記憶装置３５１１の外から供給される。

【０１０６】

図３５に示したソフトウエアの第２の利用許可証検査部３５０７も図２８に示した第１の利用許可証検査部３５０６と同様の内部構成を持ち、図２９と同様の動作を行う。

【０１０７】

図３６は、本発明を適用したデジタルコンテンツプロセッシングソフトウエアである。本ソフトウエアは、文書・画像・音楽・映像といったデジタルコンテンツに対して表示・編集・印刷が可能なソフトウエアである。本ソフトウエアでは、コンテンツに対して操作を行う前に、利用者が正しい利用許可証を持っている

かどうかが確認され、利用者が正しい利用許可証を所持する場合にのみ操作が可能である。

【０１０８】

ソフトウエア３６０１は、入出力制御部３６０２、処理制御部３６０３、表示実行部３６０４、編集実行部３６０５、印刷実行部３６０６、コンテンツデータ記憶部３６０７、利用許可証検査部３６０８からなる。

【０１０９】

それぞれの構成要素の役割を以下に示す。

【０１１０】

入出力制御部３６０２：利用者からの入力あるいは、利用者への出力を制御する。

処理制御部３６０３：入出力制御部３６０２からの利用者の命令を受け取り、命令に応じてデジタルコンテンツの表示、編集、印刷といった機能を実行する。

表示実行部３６０４：入出力制御部３６０２からの呼び出しに応じてデジタルコンテンツの表示を実行する。実行の前に利用許可証検査部３６０８を呼び出し、利用者が現在操作中のデジタルコンテンツの表示に対する正しい利用許可証を所持している事を確認する。

編集実行部３６０５：入出力制御部３６０２からの呼び出しに応じてデジタルコンテンツの編集を実行する。実行の前に利用許可証検査部３６０８を呼び出し、利用者が現在操作中のデジタルコンテンツの編集に対する正しい利用許可証を所持している事を確認する。

印刷実行部３６０６：入出力制御部３６０２からの呼び出しに応じてデジタルコンテンツの印刷を実行する。実行の前に利用許可証検査部３６０８を呼び出し、利用者が現在操作中のデジタルコンテンツの印刷に対する正しい利用許可証を所持している事を確認する。

コンテンツデータ記憶部３６０７：利用者が現在操作中のデジタルコンテンツのデータを保持する。

利用許可証検査部３６０８：表示実行部３６０４、編集実行部３６０５、印刷実行部３６０６から呼び出され、利用者が、現在操作中のデジタルコンテンツに対

して指定された操作を実行可能な利用許可証を所持しているかどうかを検査する。

【０１１１】

また、本ソフトウエアが動作するコンピュータ上には、消費者秘密情報や利用許可証を保持し、利用許可証の正当性の検査に使用する情報を作成して、利用許可証検査部３６０８に送付する利用許可証明部３６１１が存在する。

【０１１２】

図３７に本ソフトウエアが操作するデジタルコンテンツのデータ構造を示す。

【０１１３】

本ソフトウエアが操作するデジタルコンテンツは、複数のページからなる。各ページに施される操作の種類毎に検証用公開鍵が割り当てられており、各ページの各機能毎に、必要となる利用許可証が異なる。

【０１１４】

デジタルコンテンツ３７０１は、３７０２、３７０３、３７０４といったページ毎のデータに別れている。各ページデータ３７１１は、そのページの表示に割り当てられた検証用公開鍵の情報３７１２、同じページの編集に割り当てられた検証用公開鍵の情報３７１３、同じページの印刷用に割り当てられた検証用公開鍵の情報３７１４、および、そのページのデータ本体３７１５からなる。さらに各検証用公開鍵の情報３７２１は、その検証用公開鍵に割り当てられた識別子３７２２、該検証用公開鍵の法数３７２３、該検証用公開鍵の公開鍵３７２４からなる。

【０１１５】

たとえば、あるページの編集を行いたい場合に、該ページの編集用に割り当てられた検証用公開鍵に対応する利用証明証を消費者が所持しているかどうかが検査される。

【０１１６】

デジタルコンテンツの改竄を防ぐために、本ソフトウエアが操作するデジタルコンテンツにはデジタル署名が施される。デジタル署名３７０５はデジタルコンテンツ３７０１の最後尾に付属しており、該コンテンツが改竄されていないかど

うかを必要に応じて検査することができる。

【０１１７】

図３０は、図３６に示したソフトウエア３６０１の利用許可証検査部３６０８と、該ソフトウエアに対して利用許可証の正当性の検査に使用する情報を供給する利用許可証明部３６１１の内部構成を示したものである。利用許可証検査部３６０８は、チャレンジと呼ぶ乱数値を利用許可証明部３６１１に送付し、利用許可証明部３６１１は、受け取ったチャレンジからレスポンスと呼ぶ値を計算して出力し、利用許可証検査部３６０８がレスポンスの正しさを検査する事で、利用許可証明部３６１１に保持されている利用許可証の正当性を検証する。

【０１１８】

利用許可証検査部３６０８は、入出力インタフェース３００１、チャレンジ生成部３００２、条件判定対象情報生成部３００３、公開鍵情報記憶部３００４、レスポンス検査部３００５、利用条件判定部３００６、利用許可証記憶部３００７、通信制御部３００８から構成される。

【０１１９】

利用許可証検査部３６０８の各部の役割を以下に示す。

【０１２０】

入出力インタフェース３００１：表示実行部３６０４、編集実行部３６０５、印刷実行部３６０６からの入力をうけ、利用許可証の検査結果を出力するインタフェース。

チャレンジ生成部３００２：利用許可証明部３６１１に送付するチャレンジを生成する。

条件判定対象情報生成部３００３：利用許可証に記載されている利用条件が特定の条件を満たす場合にのみ機能を実行する場合、その判断の対象となる情報を生成する。

公開鍵情報記憶部３００４：利用許可証の検査に使用する検証用公開鍵に関する情報を記憶する。

レスポンス検査部３００５：利用許可証明部３６１１が作成したレスポンスの正しさを検査する。

利用条件判定部３００６：利用許可証に記載されている利用条件が満たされているかどうかを判定する。

利用許可証記憶部３００７：利用許可証明部３６１１から取り出した利用許可証を保持する。

通信制御部３００８：利用許可証明部３６１１との間の通信を制御する。

【０１２１】

また、利用許可証明部３６１１は、入出力制御部３０１１、消費者秘密情報記憶部３０１２、レスポンス計算部３０１３、利用許可証記憶部３０１４から構成される。

【０１２２】

利用許可証明部３６１１の各部の役割を以下に示す。

【０１２３】

入出力制御部３０１１：利用許可証検査部３６０８との間の通信を制御する。

消費者秘密情報記憶部３０１２：消費者秘密情報を保持する。

レスポンス計算部３０１３：利用許可証検査部３６０８に送付するレスポンスを計算する。

利用許可証記憶部３０１４：利用許可証が複数保持される。

【０１２４】

図３１は、利用許可証の検証の際の利用許可証検査部３６０８と利用許可証明部３６１１の動作を示すフローチャートである。図３１に従って利用許可証の検証の際の利用許可証検査部３６０８と利用許可証明部３６１１の動作を説明する。

【０１２５】

図３７に示したデジタルコンテンツのあるページに対して表示・編集・印刷がソフトウエアの利用者から指示された場合、表示実行部３６０４、編集実行部３６０５あるいは印刷実行部３６０６は、利用許可証検査部３６０８を呼び出して利用許可証の検査を行う。その際、表示実行部３６０４、編集実行部３６０５あるいは印刷実行部３６０６は、現在対象となっているページの、実行しようとする機能に割り当てられた検証用公開鍵の情報（検証用公開鍵識別子ＩＤ、法数ｎ

、公開鍵ｅ）をコンテンツデータ記憶部３６０７に記憶されているデジタルコンテンツから取り出して、入出力インタフェース３００１を介して利用許可証検査部３６０８に入力する。利用許可証検査部３６０８は、この入力を受けた時点から利用許可証の検査を開始する。

【０１２６】

利用許可証検査部３６０８は、まず最初に、入出力インタフェース３００１を介して入力された検証用公開鍵の情報を公開鍵情報記憶部３００４に記憶する（３１００）。

【０１２７】

次に、利用許可証検査部３６０８は、通信制御部３００８を介して利用許可証明部３６１１の利用許可証記憶部３０１４にアクセスし、利用許可証記憶部３０１４に保持されている利用許可証のうち、利用許可証の検査に使用可能なものを探す（３１０１）。利用許可証記憶部３０１４に保持されている利用許可証のうち、その公開鍵識別子フィールドの値が公開鍵情報記憶部３００４に保持されている検証用公開鍵識別子と一致するものが、求める利用許可証である。ここで該当する利用許可証が見つからなければ、利用許可証の検査は失敗であり、エラー処理の後（３１０９）、終了する。

【０１２８】

該当する利用許可証が見つかった場合には、該利用許可証が取り出され、利用許可証検査部３６０８の利用許可証記憶部３００７に記憶される（３１０２）。

【０１２９】

次に、利用条件判定部３００６で、利用許可証記憶部３００７に保持されている利用許可証に含まれる利用条件１が満たされているかどうかが判定される（３１０３）。利用条件１に記載されている利用許可証の有効期間開始や終了のチェックのために、利用条件判定部３００６は時計を内蔵している。また、条件判定対象情報生成部３００３で生成された条件判定対象情報ｓが存在する場合、条件判定対象情報ｓが利用条件１を満たすかどうかもここで判定される。

【０１３０】

３１０３で、利用条件１が満たされていないと判断された場合、利用許可証の

検査は失敗であり、エラー処理の後（３１０９）、終了する。

【０１３１】

３１０３で、利用条件１が満たされていると判断された場合、チャレンジ生成部３００２でチャレンジＣが作成される（３１０４）。チャンレンジは検証を行うたびに異なる乱数値であり、チャンレンジ生成部３００２は乱数生成機能を内包している。

【０１３２】

チャレンジが生成された後、生成されたチャレンジＣ、公開鍵情報記憶部３００４に保持されている法数ｎおよび公開鍵ｅ、利用許可証記憶部３００７に記憶されている利用許可証が含む利用条件１が、通信制御部３００８を介して利用許可証明部３６１１に送付される（３１０５）。

【０１３３】

チャレンジを受け取った利用許可証明部３６１１は、レスポンス計算部３０１３でレスポンスＲを計算し（３１０６）、通信制御部３０１１を介して利用許可証検査部３６０８に送付される（３１０７）。レスポンスＲは、通信制御部３０１１を介して利用許可証検査部３６０８から入力されたチャレンジＣ、法数ｎ、公開鍵ｅ、利用条件１、消費者秘密情報記憶部３０１３に保持されている消費者秘密情報ｕから、以下の（４）式にしたがって計算される。

【０１３４】

【数４】

$$R = C^{f(n,e,u,l)} \mod n \qquad (4)$$

通信制御部３００８を介してレスポンスＲを受け取った利用許可証検査部３６０８は、レスポンス検査部３００５でレスポンスＲの正当性を検査する（３１０８）。検証にはレスポンスＲの他に、チャレンジ生成部３００２が生成したチャレンジＣ、公開鍵情報記憶部３００４が記憶している法数ｎ、公開鍵ｅ、利用許可証記憶部３００７が保持している利用許可証に含まれる証明値ｔが使用される。（５）の式が成り立てば検証成功、そうでなければ失敗である。

【０１３５】

【数５】

$C \equiv (C^{t}R)^{e} \mod n$　　（５）

（１）（４）（５）の式からわかるように、法数や公開鍵、証明値、利用条件、消費者秘密情報の組み合わせが正しい時のみレスポンスの検査に成功する。検証用公開鍵が異なるデジタルコンテンツの利用許可証を流用したり、他人の利用許可証を利用したり、利用条件を改竄したりといった攻撃は困難である。

【０１３６】

前述したように、利用条件１には、利用許可証の有効期間以外に多くの条件が記載可能である。たとえば、利用可能な回数を利用条件１に指定することは好適な例である。この場合、条件判定対象情報生成部３００３に現在までの使用回数を保持する機構を設けておき、３１０３の判断の際に条件判定対象情報ｓとして利用条件判定部３００６に送付し、そこで利用条件１に記載されている利用可能な回数と比較すればよい。

【０１３７】

編集のように長時間かかる作業の際は、編集作業の開始時に利用許可証の検査に成功したとしても、編集作業の途中で利用許可証の有効期間が切れてしまうことがありえる。このような場合には、数分毎に、利用許可証の検査をおこない、利用許可証の有効期間が切れていることがわかった場合には、その時点で編集が実行できなくなるように構成すればよい。

【０１３８】

デジタルコンテンツに含まれるデータ本体３７１５が、特に暗号化等の施されていない形式であった場合、デジタルコンテンツのファイルからデータ本体のみを取り出すことで、利用許可証の検査なしに、デジタルコンテンツの内容にアクセスできる可能性がある。これを防ぐためには、データ本体３７１５には暗号化されたデータを入れておけばよい。利用許可証の検査に成功した場合にのみ一時的に復号し、各種機能を実行するようにすることで、ファイルからデジタルコンテンツの内容が漏れることを防ぐことができる。

【０１３９】

図３８は、本発明を適用したデジタルコンテンツを復号するソフトウエアである。本ソフトウエアは、暗号化された状態で存在する文書・画像・音楽・映像と

いったデジタルコンテンツを復号して利用可能な形式として出力するものである、復デジタルコンテンツの復号には利用許可証が必要であり、本ソフトウエアは、復号を実行する前に、本ソフトウエアの利用者が正しい利用許可証を所持しているかどうかを検査する。

【０１４０】

ソフトウエア３８０１は、入出力制御部３８０２、復号部３８０３、利用許可証検査部３８０４からなる。

【０１４１】

それぞれの構成要素の役割を以下に示す。

【０１４２】

入出力制御部３８０２：利用者からの入力あるいは、利用者への出力を制御する。

復号部３８０３：暗号化されているデジタルコンテンツを復号する。

利用許可証検査部３８０４：復号部３８０３から呼び出され、利用者が、現在操作中のデジタルコンテンツを復号可能な利用許可証を所持しているかどうかを検査する。

【０１４３】

また、本ソフトウエアが動作するコンピュータ上には、消費者秘密情報や利用許可証を保持し、利用許可証の正当性の検査に必要な情報を利用許可証検査部３８０４に送付する利用許可証明部３８１１が存在する。

【０１４４】

図３９に本ソフトウエアが復号するデジタルコンテンツのデータ構造を示す。

【０１４５】

本ソフトウエアが復号するデジタルコンテンツ３９０１は、暗号化されたデータ本体３９０３と、本デジタルコンテンツの復号に割り当てられた検証用公開鍵の情報３９０２、さらには、データ本体３９０３と検証用公開鍵の情報３９０２に対するデジタル署名３９０４からなる。デジタル署名３９０４は、デジタルコンテンツの改竄を防ぐためのものである。デジタルコンテンツ３９０１の最後尾に付属しており、デジタルコンテンツ３９０１が改竄されていないかどうかを必

要に応じて検査することができる。

【０１４６】

図３２は、図３８に示したソフトウエア３８０１の利用許可証検査部３８０４と、該ソフトウエアに対して利用許可証の正当性の検査に使用する情報を供給する利用許可証明部３８１１の内部構成を示したものである。利用許可証検査部３６０８は、利用許可証明部３８１１が保持している利用許可証をとりだし、その正当性を検証する。

【０１４７】

利用許可証検査部３８０４は、入出力インタフェース３２０１、条件判定対象情報生成部３２０２、利用条件判定部３２０３、公開鍵情報記憶部３２０４、証明値検査部３２０５、利用許可証記憶部３２０６、通信制御部３２０７、消費者秘密情報記憶部３２０８から構成される。

【０１４８】

利用許可証検査部３８０４の各部の役割を以下に示す。

【０１４９】

入出力インタフェース３２０１：復号部３８０３からの入力をうけ、利用許可証の検査結果を出力するインタフェース。

条件判定対象情報生成部３２０２：利用許可証に記載されている利用条件が特定の条件を満たす場合にのみデジタルコンテンツを復号する場合、その判断の対象となる情報を生成する。

利用条件判定部３２０３：利用許可証に記載されている利用条件が満たされているかどうかを判定する。

公開鍵情報記憶部３２０４：利用許可証の検査に使用する検証用公開鍵に関する情報を記憶する。

証明値検査部３２０５：利用許可証に記載されている証明値の正当性を検査する。

利用許可証記憶部３２０６：利用許可証明部３８１１から取り出した利用許可証を保持する。

通信制御部３２０７：利用許可証明部３８１１との間の通信を制御する。

消費者秘密情報記憶部３２０８：利用許可証明部３８１１から取り出した消費者秘密情報を保持する。

【０１５０】

また、利用許可証明部３８１１は、通信制御部３２１１、消費者秘密情報記憶部３２１２、利用許可証記憶部３２１３から構成される。

【０１５１】

利用許可証明部３８１１の各部の役割を以下に示す。

【０１５２】

通信制御部３２１１：利用許可証検査部３８０４との間のデータの入出力を制御する。

消費者秘密情報記憶部３２１２：消費者秘密情報を保持する。

利用許可証記憶部３２１３：利用許可証が複数保持される。

【０１５３】

図３３は、利用許可証の検証の際の利用許可証検査部３８０４と利用許可証明部３８１１の動作を示すフローチャートである。図３３に従って利用許可証の検査の際の利用許可証検査部３８０４と利用許可証明部３８１１の動作を説明する。

【０１５４】

図３９に示したデジタルコンテンツの復号が利用者から指示された場合、復号部３８０３は、利用許可証検査部３８０４を呼び出して利用許可証の検証を行う。その際復号部３８０３は、該デジタルコンテンツに付随している検証用公開鍵の情報（検証用公開鍵識別子ＩＤ、法数ｎ、公開鍵ｅ）を取り出して、入出力インタフェース３２０１を介して利用許可証検査部３８０４に入力する。利用許可証検査部３８０４は、この入力を受けた時点から利用許可証の検査を開始する。

【０１５５】

利用許可証検査部３８０４は、まず、入出力インターフェース３２０１を介して入力された検証用公開鍵の情報を公開鍵情報記憶部３２０４に記憶する（３３００）。次に通信制御部３２０７を介して利用許可証明部３８１１の利用許可証記憶部３２１３にアクセスし、利用許可証記憶部３２１３に保持されている利用

許可証のうち、利用許可証検査部３８０４による利用許可証の検査に使用可能なものを探す（３３０１）。利用許可証記憶部３２１１に保持されている利用許可証のうち、その公開鍵識別子フィールドの値が公開鍵情報記憶部３２０４に保持されている検証用公開鍵識別子と一致するものが、求める利用許可証である。ここで該当する利用許可証が見つからなければ、利用許可証の検査は失敗であり、エラー処理の後（３３０６）、終了する。

【０１５６】

該当する利用許可証が見つかった場合には、該利用許可証が取り出され、利用許可証検査部３８０４の利用許可証記憶部３２０６に記憶される（３３０２）。

【０１５７】

次に、利用条件判定部３２０３で、利用許可証記憶部３２０６に保持されている利用許可証に含まれる利用条件１が満たされているかどうかが判定される（３３０３）。利用条件１に記載されている利用許可証の有効期間開始や終了のチェックのために、利用条件判定部３２０３は時計を内蔵している。また、条件判定対象情報生成部３２０２で生成された条件判定対象情報ｓが存在する場合、条件判定対象情報ｓが利用条件１を満たすかどうかもここで判定される。

【０１５８】

３３０３で、利用条件１が満たされていないと判断された場合、利用許可証の検査は失敗であり、エラー処理の後（３３０６）、終了する。

【０１５９】

３３０３で、利用条件１が満たされていると判断された場合、通信制御部３２０７を介して利用許可証明部３８１１の消費者秘密情報記憶部３２１２にアクセスし、消費者秘密情報記憶部３２１２に保持されている消費者秘密情報ｕを取り出し、利用許可証検査部３８０４の消費者秘密情報記憶部３２０８に記憶する（３３０４）。

【０１６０】

最後に、証明値検査部３２０５で、利用許可証記憶部３２０６に保持されている利用許可証に含まれる証明値ｔの正当性を検査する（３３０５）。検証のために、証明値検査部３２０５は乱数ｒを生成し、公開鍵情報記憶部３２０４が記憶

している法数ｎ、公開鍵ｅ、利用許可証記憶部３２０６が保持している利用許可証に含まれる利用条件１、消費者秘密情報記憶部３２０８が保持している消費者秘密情報ｕに対して　（６）の式が成り立つかどうかを検査する。

【０１６１】

【数６】

$$r \equiv (r^{t+f(n,e,u,l)})^{e} \mod n \qquad (6)$$

（１）（６）の式からわかるように、法数や公開鍵、証明値、利用条件、消費者秘密情報の組み合わせが正しい時のみ証明値の検査に成功する。検証用公開鍵が異なるデジタルコンテンツの利用許可証を流用したり、他人の利用許可証を利用したり、利用条件を改竄したりといった攻撃は困難である。

【０１６２】

圧縮されたデジタルコンテンツを伸長する際に、伸長のための利用許可証の検査をするよう構成する場合も、図３８に示したソフトウエアと同様の構成と動作が利用できる。暗復号の処理がが圧縮伸長の処理に変わるだけで、構成や動作はまったく同じものが利用できる。

【０１６３】

図３５に示したソフトウエアや、図３７、図３９に示したようなファイルといったデジタルコンテンツは、利用許可証を持たない消費者は使用できないので、消費者は、デジタルコンテンツ自体をいかなる流通経路を使って入手してもかまわない。したがって、デジタルコンテンツの提供者は、消費者にとって便利な様々な経路でデジタルコンテンツを配布することができる。たとえば、インターネット上の特定のサイトからのダウンロードでもよいし、ＣＤ－ＲＯＭ等に記憶させて配布するのでもよい。衛星放送でデジタルコンテンツを放送してもよいし、デジタルコンテンツのコピーを友人同士で交換してもかまわない。

【０１６４】

［検証用公開鍵情報の発行］

検証用公開鍵情報はプロバイダからの依頼によって、センタで作成され、依頼したプロバイダに送付される。依頼の際には、検証用公開鍵情報依頼というデータが送受信される。通常、発信者は依頼をするプロバイダであり受信者は依頼を

受けるセンタであるが、インターネットに接続されたその他のエンティティがプロバイダの代わりに依頼を行ったりセンタの代わりに依頼を受けたりする場合には、プロバイダやセンタ以外のエンティティが発信者や受信者になってもよい。

【０１６５】

検証用公開鍵情報依頼のデータ構造を以下に示す。

【０１６６】

【表４】

検証用公開鍵情報依頼：：＝｛

発信者フィールド，

受信者フィールド，

日時フィールド，

公開鍵仕様フィールド，

デジタル署名フィールド，

証明証フィールド

｝

【０１６７】

発信者フィールド：この検証用公開鍵情報依頼の発信者の識別子が記載される。発信者は通常プロバイダであるが、インターネットに接続された別のエンティティでもよい。

受信者フィールド：この検証用公開鍵情報依頼の受信者の識別子が記載される。受信者は通常センタであるが、インターネットに接続された別のエンティティでもよい。

日時フィールド：この検証用公開鍵情報依頼の作成日時が記載される。

公開鍵仕様フィールド：作成してもらう検証用公開鍵に対する依頼者の要望が記載される。検証用公開鍵を使用するプロバイダの識別子、公開鍵暗号アルゴリズム、鍵長の情報がここに記述できる。

デジタル署名フィールド：この検証用公開鍵情報依頼の発信者によるこの検証用公開鍵情報依頼に対するデジタル署名が記載される。

証明証フィールド：この検証用公開鍵情報依頼のデジタル署名フィールドのデジ

タル署名を検証するための公開鍵を含む公開鍵証明証群が記載される。

【０１６８】

検証用公開鍵情報依頼を受け取ったセンタは、検証用公開鍵情報依頼に記載された公開鍵仕様にしたがって公開鍵ペアを作成し、検証用公開鍵情報を作成して依頼者に渡す。依頼された検証用公開鍵情報を作成するかしないか、あるいは、指定された公開鍵仕様通りに公開鍵を作成するかどうかはセンタが決定できる。

【０１６９】

検証用公開鍵情報を引き渡す際には、検証用公開鍵情報送付というデータが送受信される。通常、発信者は検証用公開鍵情報を作成したセンタであり、受信者は発行された検証用公開鍵情報を使用するプロバイダであるが、インターネットに接続されたその他のエンティティがセンタの代わりに検証用公開鍵情報の送付を行ったり、プロバイダの代わりに検証用公開鍵情報を受け取ったりする場合には、センタやプロバイダ以外のエンティティが発信者や受信者になってもよい。

【０１７０】

検証用公開鍵情報送付のデータ構造を以下に示す。

【０１７１】

【表５】

検証用公開鍵情報送付：：＝｛
発信者フィールド，
受信者フィールド，
日時フィールド，
検証用公開鍵情報フィールド，
デジタル署名フィールド，
証明証フィールド
｝

【０１７２】

発信者フィールド：この検証用公開鍵情報送付の送付者の識別子が記載される。発信者は通常センタであるが、インターネットに接続された別のエンティティでもよい。

受信者フィールド：この検証用公開鍵情報送付の受信者の識別子が記載される。受信者は通常プロバイダであるが、インターネットに接続された別のエンティティでもよい。

日時フィールド：この検証用公開鍵情報送付の作成日時が記載される。

検証用公開鍵情報フィールド：この検証用公開鍵情報送付で送られる検証用公開鍵情報が記載される。

デジタル署名フィールド：この検証用公開鍵情報送付の発信者によるこの検証用公開鍵情報送付に対するデジタル署名が記載される。

証明証フィールド：この検証用公開鍵情報送付のデジタル署名フィールド、およびこの検証用公開鍵情報送付に含まれる検証用公開鍵情報のデジタル署名フィールドのデジタル署名を検証するための公開鍵を含む公開鍵証明証群が記載される。

【０１７３】

［利用許可証仲介許諾］

本実施例では、プロバイダとリテーラは独立に存立することが可能である。リテーラは多様なプロバイダが提供する多様なデジタルコンテンツの販売を行うことが可能であるし、特定のプロバイダが自己の提供するデジタルコンテンツを多くのリテーラに販売をしてもらうといったことも可能である。

【０１７４】

プロバイダにとっては、多くのリテーラに自己のデジタルコンテンツを販売してもらうことは基本的には有利であるが、信用度の低いリテーラに販売をされるのは、後のトラブルを招く可能性が高く許容できない。したがって、プロバイダは自己のデジタルコンテンツを取り扱えるリテーラをコントロールする必要がある。

【０１７５】

このコントロール可能にするために、本実施例では利用許可証仲介許諾というデータを使用する。

【０１７６】

利用許可証仲介許諾はプロバイダが特定のリテーラに対して自己の特定のデジ

タルコンテンツの販売を委託している事を証するデジタルデータであり、リテーラからの依頼を受けて作成され、依頼者に送付される。

【０１７７】

以降、単に仲介許諾といえば利用許可証仲介許諾を、仲介許諾証といえば利用許可証仲介許諾証を指すものとする。

【０１７８】

仲介許諾証のデータ構造を以下に示す。

【０１７９】

【表６】

仲介許諾証：：＝｛

発行者フィールド，
受領者フィールド，
発行日フィールド，
仲介許諾識別子フィールド，
有効期間開始日時フィールド，
有効期間終了日時フィールド，
公開鍵鍵識別子フィールド，
利用条件限定情報フィールド，
デジタル署名フィールド

｝

【０１８０】

発行者フィールド：この仲介許諾証の発行者であるプロバイダの識別子が記載される。

受領者フィールド：この仲介許諾証の受領者であるリテーラの識別子が記載される。

発行日フィールド：この仲介許諾証の発行日が記載される。

仲介許諾識別子フィールド：この仲介許諾証にプロバイダが割り当てた識別子が記載される。

有効期間開始日時フィールド：この仲介許諾証の有効期間の開始日時が記載され

る。

有効期間終了日時フィールド：この仲介許諾証の有効期間の終了日時が記載される。

公開鍵識別子フィールド：この仲介許諾証によって利用許可証の仲介が許諾される検証用公開鍵に割り当てられた検証用公開鍵識別子が記載される。

利用条件限定情報フィールド：利用許可証に記載される利用条件の範囲を限定する情報である利用条件限定情報が記載される。

デジタル署名フィールド：発行者であるプロバイダによるこの仲介許諾証全体に対するデジタル署名が記載される。

【０１８１】

利用条件限定情報フィールドに記載される利用条件限定情報によって、プロバイダはリテーラの仲介によって発行される利用許可証に記載される利用条件を詳細にコントロールする事ができる。

【０１８２】

利用条件限定情報のデータ構造を以下に示す。

【０１８３】

【表７】

利用条件限定情報：：＝｛

最短有効期間フィールド，

最長有効期間フィールド，

・・・

｝

【０１８４】

最短有効期間フィールド：この仲介許諾証の受領者であるリテーラが仲介して発行される、この仲介許諾証の公開鍵鍵識別子フィールドに指定された検証用公開鍵に対応する利用許可証の利用条件フィールドに記載される有効期間開始から有効期間終了までの間の長さの最低限度が記載される。該利用許可証の利用条件フィールドに記載される有効期間開始から有効期間終了までの間の長さは、ここに記載される値以上でなければならない。

最長有効期間フィールド：この仲介許諾証の受領者であるリテーラが仲介して発行される、この仲介証の公開鍵鍵識別子フィールドに指定された検証用公開鍵に対応する利用許可証の利用条件フィールドに記載される有効期間開始から有効期間終了までの間の長さの最長限度が記載される。該利用許可証の利用条件フィールドに記載される有効期間開始から有効期間終了までの間の長さは、ここに記載される値以下でなければならない。

【０１８５】

利用条件限定情報には、最短有効期間あるいは最長有効期間以外にも、この仲介許諾証の公開鍵鍵識別子フィールドで指定された検証用公開鍵とバインドされているデジタルコンテンツに応じて種々の限定を設定する事が可能である。

【０１８６】

例えば、デジタルコンテンツの利用回数が特定の回数以下に限定されるような場合、最小利用可能回数や最大利用可能回数を利用条件限定情報に記載しておき、その範囲内で利用条件に利用可能回数を指定するように構成する。

【０１８７】

また、デジタルコンテンツの利用時にいくらかの料金を課金あるいは徴収するために利用条件にその金額を指定する場合には、指定可能な金額の範囲を利用条件限定情報に記載する。

【０１８８】

さらに、デジタルコンテンツが持つ機能のうちの特定の機能の利用のみを許すために利用条件にその機能を指定する場合には、指定可能な機能の範囲を利用条件限定情報に記載する。

【０１８９】

［仲介許諾証の発行］

仲介許諾証はリテーラからの依頼によって、プロバイダで作成され、依頼したリテーラに送付される。依頼の際には、仲介許諾証依頼というデータが送受信される。通常、発信者は依頼をするリテーラであり受信者は依頼を受けるプロバイダであるが、インターネットに接続されたその他のエンティティがリテーラの代わりに依頼を行ったりプロバイダの代わりに依頼を受けたりする場合には、リテ

ーラやプロバイダ以外のエンティティが発信者や受信者になってもよい。

【０１９０】

仲介許諾証依頼のデータ構造を以下に示す。

【０１９１】

【表８】

仲介許諾証依頼：：＝｛

発信者フィールド，

受信者フィールド，

日時フィールド，

仲介許諾仕様フィールド，

デジタル署名フィールド，

証明証フィールド

｝

【０１９２】

発信者フィールド：この仲介許諾証依頼の発信者の識別子が記載される。発信者は通常リテーラであるが、インターネットに接続された別のエンティティでもよい。

受信者フィールド：この仲介許諾証依頼の受信者の識別子が記載される。受信者は通常プロバイダであるが、インターネットに接続された別のエンティティでもよい。

日時フィールド：この仲介許諾証依頼の作成日時が記載される。

仲介許諾仕様フィールド：作成してもらう仲介許諾証に対する依頼者の要望を記載した仲介許諾仕様が記載される。

デジタル署名フィールド：この仲介許諾証依頼の発信者によるこの仲介許諾証依頼に対するデジタル署名が記載される。

証明証フィールド：この仲介許諾証依頼のデジタル署名フィールドのデジタル署名を検証するための公開鍵を含む公開鍵証明証群が記載される。

【０１９３】

仲介許諾証依頼の仲介許諾仕様フィールドに記載される仲介許諾仕様のデータ

構造を以下に示す。

【０１９４】

【表９】

仲介許諾仕様：：＝｛

許諾者フィールド，

被許諾者フィールド，

公開鍵識別子フィールド，

希望利用条件限定情報フィールド

｝

【０１９５】

許諾者フィールド：仲介許諾証を作成してほしいプロバイダの識別子が記載される。

被許諾者フィールド：希望する仲介許諾証によって許諾を受けるリテーラの識別子が記載される。

公開鍵鍵識別子フィールド：仲介許諾証で利用許可証の仲介を許諾してほしい検証用公開鍵に割り当てられた検証用公開鍵識別子が記載される。

希望利用条件限定情報フィールド：作成してもらう仲介許諾証に記載してほしい利用条件限定情報が記載される。

【０１９６】

仲介許諾証依頼を受け取ったプロバイダは、仲介許諾証依頼に記載された仲介許諾仕様にしたがって仲介許諾証を作成し、リテーラに渡す。依頼された仲介許諾証を作成するかしないか、あるいは、指定された仲介許諾仕様どおりに仲介許諾証を作成するかどうかはプロバイダが決定できる。

【０１９７】

作成した仲介許諾証を引き渡す際には、仲介許諾証送付というデータが送受信される。通常、発信者は仲介許諾証を作成したプロバイダであり、受信者は発行された仲介許諾証を使用するリテーラであるが、インターネットに接続されたその他のエンティティがプロバイダの代わりに仲介許諾証の送付を行ったり、リテーラの代わりに仲介許諾証を受け取ったりする場合には、プロバイダやリテーラ

以外のエンティティが発信者や受信者になってもよい。

【０１９８】

仲介許諾証送付のデータ構造を以下に示す。

【０１９９】

【表１０】

仲介許諾証送付：：＝｛

発信者フィールド，

受信者フィールド，

日時フィールド，

仲介許諾証フィールド，

デジタル署名フィールド，

証明証フィールド

｝

【０２００】

発信者フィールド：この仲介許諾証送付の送付者の識別子が記載される。発信者は通常プロバイダであるが、インターネットに接続された別のエンティティでもよい。

受信者フィールド：この仲介許諾証送付の受信者の識別子が記載される。受信者は通常リテーラであるが、インターネットに接続された別のエンティティでもよい。

日時フィールド：この仲介許諾証送付の作成日時が記載される。

仲介許諾証フィールド：この仲介許諾証送付で送られる仲介許諾証が記載される。

デジタル署名フィールド：この仲介許諾証送付の発信者によるこの仲介許諾証送付に対するデジタル署名が記載される。

証明証フィールド：この仲介許諾証送付のデジタル署名フィールド、およびこの仲介許諾証送付に含まれる仲介許諾証のデジタル署名フィールドのデジタル署名を検証するための公開鍵を含む公開鍵証明証群が記載される。

【０２０１】

［利用許可証の発行］

利用許可証は、消費者からの依頼に応じて発行される。消費者はリテーラに対して特定のデジタルコンテンツに対して特定の利用条件での予約を依頼する利用許可証依頼を送付する。利用許可証依頼を受け取ったリテーラは、通常センタに対して、依頼元である消費者に対する利用許可証の発行を依頼するため利用許可証依頼を作成し、センタに送付する。利用許可証依頼を受け取ったセンタは消費者向けの利用許可証を作成し、利用許可証依頼を送付してきたリテーラに渡す。利用許可証を受け取ったリテーラは、その利用許可証をその依頼者である消費者に送付する。センタからあるいはリテーラからの利用許可証の送付には、利用許可証送付というデータが送受信される。

【０２０２】

消費者とセンタの間を複数のリテーラが仲介することも可能である。その場合、消費者からの依頼を直接受けたリテーラが第２のリテーラに利用許可証依頼を送付し、第２のリテーラがセンタに利用許可証依頼を送付するという形態をとる。発行された利用許可証は逆の経路で利用許可証送付を送付していく事で消費者に届いてもよいし、いくつかのリテーラをスキップしてもよい。

【０２０３】

利用許可証依頼のデータ構造を以下に示す。

【０２０４】

【表１１】

利用許可証依頼：：＝｛
　　発信者フィールド，
　　受信者フィールド，
　　日時フィールド，
　　許可内容フィールド，
　　デジタル署名フィールド，
　　証明証フィールド
　　｝

【０２０５】

発信者フィールド：この利用許可証依頼の発信者の識別子が記載される。

受信者フィールド：この利用許可証依頼の受信者の識別子が記載される。

日時フィールド：この利用許可証依頼の作成日時が記載される。

許可内容フィールド：依頼する利用許可証の内容に関する要望のためのフィールドである。通常、利用許可に関する要望を記した許可仕様が記載されるが、受信者がリテーラであって、リテーラで販売している物品あるいはサービスにリテーラ独自の管理番号が割り当ててある場合には、その番号が記載されることもある。

デジタル署名フィールド：この利用許可証依頼の発信者によるこの利用許可証依頼に対するデジタル署名が記載される。

証明証フィールド：この利用許可証依頼のデジタル署名フィールド、およびこの利用許可証依頼に仲介許諾が含まれるならばそのデジタル署名フィールドのデジタル署名を検証するための公開鍵を含む公開鍵証明証群が記載される。

【０２０６】

利用許可証依頼の許可内容フィールドに記載される許可仕様のデータ構造を以下に示す。

【０２０７】

【表１２】

```
許可仕様：：＝｛
            公開鍵識別子フィールド，
            消費者識別子フィールド，
            利用条件フィールド，
            仲介許諾証フィールド
            ｝
```

【０２０８】

【表１３】

公開鍵鍵識別子フィールド：利用許可証依頼で依頼する利用許可証を検証できる検証用公開鍵に割り当てられた検証用公開鍵識別子が記載される。

消費者識別子フィールド：利用許可証依頼で依頼する利用許可証で予約を証され

る消費者の識別子が記載される。

利用条件フィールド：利用許可証依頼で依頼する利用許可証に記載してほしい利用条件が記載される。

仲介許諾証フィールド：利用許可証依頼の発信者がリテーラの場合に、そのリテーラが、この許可仕様の公開鍵鍵識別子フィールドに指定された識別子をもつ検証用公開鍵に対応する利用許可証を、この許可仕様の利用条件フィールドに記載された利用条件で仲介することが許諾されている事を証する仲介許諾証が含まれる。

【０２０９】

許可仕様の利用条件フィールドに記載されたとおりの利用条件を持つ利用許可証を発行するかどうかは、センタが決定する。特に、許可仕様に含まれる仲介許諾証で許諾されていない依頼に対しては、利用許可証を発行しない。

【０２１０】

また、利用許可証の依頼の過程で、仲介するリテーラが許可仕様の利用条件フィールドの内容を修正する事もありうる。

【０２１１】

利用許可証送付のデータ構造を以下に示す。

【０２１２】

【表１４】

利用許可証送付：：＝｛

発信者フィールド，

受信者フィールド，

日時フィールド，

利用許可証フィールド，

デジタル署名フィールド，

証明証フィールド

｝

【０２１３】

発信者フィールド：この利用許可証送付の送付者の識別子が記載される。

受信者フィールド：この利用許可証送付の受信者の識別子が記載される。
日時フィールド：この利用許可証送付の作成日時が記載される。
利用許可証フィールド：この利用許可証送付で送られる利用許可証が記載される。
デジタル署名フィールド：この利用許可証送付の発信者によるこの仲介許諾送付に対するデジタル署名が記載される。
証明証フィールド：この利用許可証送付のデジタル署名フィールド、およびこの利用許可証送付に含まれる利用許可証のデジタル署名フィールドのデジタル署名を検証するための公開鍵を含む公開鍵証明証群が記載される。

【０２１４】

［センタの構成］

本実施例のセンタは、インターネットを介して入力される検証用公開鍵情報依頼と利用許可証依頼を処理する機能、利用許可証の発行履歴を作成してインターネットを介してプロバイダあるいはリテーラに送付する機能、検証用公開鍵情報の発行履歴を作成してインターネットを介してプロバイダに送付する機能を持つ。

【０２１５】

図２は、本実施例のセンタの構成図である。

【０２１６】

センタは、入出力制御部２０１、処理選択部２０２、検証用公開鍵情報依頼処理部２０３、利用許可証依頼処理部２０４、プロバイダＤＢ２０５、公開鍵ペアＤＢ２０６、リテーラＤＢ２０７、消費者ＤＢ２０８、利用許可証発行履歴ＤＢ２０９、署名鍵記憶部２１０、証明証記憶部２１１、利用許可証発行プロバイダ用履歴作成部２１２、利用許可証発行リテーラ用履歴作成部２１３、検証用公開鍵情報発行履歴作成部２１４から構成され、入出力制御部２０１を介してインターネットに接続されている。

【０２１７】

本実施例のセンタの各部の役割を以下に述べる。

【０２１８】

入出力制御部２０１：インターネットを介したデータの入力を受け付けるとともに、検証用公開鍵情報依頼処理部２０３が作成したデータや利用許可証依頼処理部２０４が作成したデータをインターネットを介して出力する。インターネットからの入出力制御部２０１への入力、あるいは、入出力制御部２０１からインターネットへの出力の方法としては、入出力制御部２０１と接続されたＷＷＷサイトを準備してプロバイダやリテーラにアクセスさせるもの、あるいは電子メールシステムと入出力制御部２０１を自動的にあるいは人手によって連動させるものなどが使用できる。

処理選択部２０２：入力したデータが検証用公開鍵情報依頼かまたは利用許可証依頼かを判断し、検証用公開鍵情報依頼であれば検証用公開鍵情報依頼処理部２０３を、利用許可証依頼であれば利用許可証依頼処理部２０４を呼び出す。

検証用公開鍵情報依頼処理部２０３：検証用公開鍵情報依頼を処理し、検証用公開鍵情報依頼送付を作成して入出力制御部２０１を介して依頼者に送付する。検証用公開鍵情報依頼送付作成の過程で、プロバイダＤＢ２０５を参照し、公開鍵ペアＤＢ２０６に新しいエントリを追加する。

利用許可証依頼処理部２０４：利用許可証依頼を処理し、利用許可証依頼送付を作成して入出力制御部２０１を介して依頼者に送付する。利用許可証依頼送付作成の過程で、公開鍵ペアＤＢ２０６、リテーラＤＢ２０７、消費者ＤＢ２０８を参照し、利用許可証発行履歴ＤＢ２０９に新しいエントリを追加する。

プロバイダＤＢ２０５：プロバイダに関するデータを保持するＤＢ。

公開鍵ペアＤＢ２０６：利用許可証の作成に使用される公開鍵ペアに関する情報を保持するＤＢ。

リテーラＤＢ２０７：リテーラに関するデータを保持するＤＢ。

消費者ＤＢ２０８：消費者に関するデータを保持するＤＢ。

利用許可証発行履歴ＤＢ２０９：利用許可証の発行履歴に関するデータを保持するＤＢ。

署名鍵記憶部２１０：センタが作成するデジタル署名に使用する署名鍵を保持する。

証明証記憶部２１１：署名鍵記憶部２１０に記憶されている署名鍵で作成したデ

ジタル署名を検証できる検証鍵を含む公開鍵証明証を保持する。
利用許可証発行プロバイダ用履歴作成部２１２：各プロバイダ毎の利用許可証の発行履歴を作成し、入出力制御部２０１を介してプロバイダに送付する。
利用許可証発行リテーラ用履歴作成部２１３：各リテーラ毎の利用許可証の発行履歴を作成し、入出力制御部２０１を介してリテーラに送付する。
検証用公開鍵情報発行履歴作成部２１４：各プロバイダ毎の検証用公開鍵情報の発行履歴を作成し、入出力制御部２０１を介してプロバイダに送付する。

【０２１９】

［センタが持つデータベース］

センタは、プロバイダＤＢ２０５、公開鍵ペアＤＢ２０６、リテーラＤＢ２０７、消費者ＤＢ２０８、利用許可証発行履歴ＤＢ２０９の５つのデータベースを持っている。

【０２２０】

プロバイダＤＢ２０５は、センタがプロバイダとして認めているエンティティに関する情報を保持したデータベースである。

【０２２１】

プロバイダＤＢ２０５の構造を図６に示す。プロバイダＤＢ２０５は以下の唯一の属性からなるテーブルである。

【０２２２】

【表１５】

プロバイダ識別子属性：センタがプロバイダとして認めているエンティティの識別子。

【０２２３】

センタは、このデータベースに登録されているプロバイダ以外のエンティティをプロバイダとは認めない。したがって、そのようなエンティティに対して検証用公開鍵情報を発行することはないし、そのようなエンティティが提供しているデジタルコンテンツに対する利用許可証を発行する事もない。

【０２２４】

センタがプロバイダと認めるエンティティを増やしたい場合には、このデータ

ベースに新規エントリを追加する。

【０２２５】

公開鍵ペアＤＢ２０６は、プロバイダに発行される検証用公開鍵と、それに対応する秘密鍵に関する情報を保持したデータベースである。本実施例では、検証用公開鍵とそれに対応する秘密鍵のための公開鍵暗号アルゴリズムとしてＲＳＡを使用する。したがって、公開鍵ペアＤＢ２０６はＲＳＡの公開鍵ペアについての情報を保持するデータベースである。

【０２２６】

公開鍵ペアＤＢ２０６の構造を図７に示す。公開鍵ペアＤＢ２０６は以下の７つの属性からなるテーブルであり、各エントリはそれぞれ一つの公開鍵ペアに関する情報である。

【０２２７】

【表１６】

公開鍵識別子属性：このエントリの公開鍵ペアに割り当てられた検証用公開鍵識別子。

法数属性：ＲＳＡ法数。

公開鍵属性：ＲＳＡ公開鍵。

秘密鍵属性：ＲＳＡ秘密鍵。

プロバイダ識別子属性：このエントリの公開鍵ペアの公開鍵を含む検証用公開鍵情報を発行されたプロバイダの識別子。

有効期間開始属性：このエントリの公開鍵ペアの公開鍵を含む検証用公開鍵情報の有効期間の開始日時。

有効期間終了属性：このエントリの公開鍵ペアの公開鍵を含む検証用公開鍵情報の有効期間の終了日時。

発行日属性：このエントリの公開鍵ペアの公開鍵を含む検証用公開鍵情報の発行日時。

【０２２８】

リテーラＤＢ２０７は、センタがリテーラとして認めているエンティティに関する情報を保持したデータベースである。

【０２２９】

リテーラＤＢ２０７の構造を図８に示す。リテーラＤＢ２０７は以下の唯一の属性からなるテーブルである。

【０２３０】

【表１７】

リテーラ識別子属性：センタがリテーラとして認めているエンティティの識別子。

【０２３１】

センタは、このデータベースに登録されているリテーラ以外のエンティティをリテーラとは認めない。したがって、そのようなエンティティからの利用許可証発行依頼に対して利用許可証を発行する事はない。

【０２３２】

センタがリテーラと認めるエンティティを増やしたい場合には、このデータベースに新規エントリを追加する。

【０２３３】

消費者ＤＢ２０８は、センタが消費者として認めているエンティティに関する情報を保持したデータベースである。

【０２３４】

消費者ＤＢ２０８の構造を図９に示す。消費者ＤＢ２０８は以下の２つの属性からなるテーブルである。

【０２３５】

【表１８】

消費者識別子属性：センタが消費者として認めている消費者識別子。

消費者秘密情報属性：消費者識別子属性で指定された消費者識別子に対応する消費者秘密情報。

【０２３６】

利用許可証発行履歴ＤＢ２０９は、センタがこれまでに発行した利用許可証に関する情報を保持したデータベースである。

【０２３７】

利用許可証発行履歴ＤＢ２０９の構造を図１０に示す。消費者ＤＢ２０８は以下の６つの属性からなるテーブルであり、各エントリはそれぞれ一つの利用許可証に関する情報である。

【０２３８】

【表１９】

公開鍵識別子属性：このエントリの利用許可証を検証できる検証用公開鍵に割り当てられた検証用公開鍵識別子。

プロバイダ識別子属性：このエントリの公開鍵識別子属性で指定された検証用公開鍵を含む検証用公開鍵情報の発行を受けたプロバイダの識別子。

消費者識別子属性：このエントリの利用許可証でデジタルコンテンツの利用を許可された消費者の消費者識別子。

仲介者識別子属性：このエントリの利用許可証の発行を依頼したリテーラの識別子。

利用条件属性：このエントリの利用許可証に記載された利用条件をＢＥＲ（Ｂａｓｉｃ　Ｅｎｃｏｄｉｎｇ　Ｒｕｌｅ：ＩＴＵ－Ｔ　Ｒｅｃｏｍｅｎｄａｔｉｏｎ　Ｘ．６９０）にしたがってエンコードした結果。

発行日属性：このエントリの利用許可証の発行日時。

【０２３９】

図３は、本実施例のセンタの動作を示すフローチャートである。本実施例のセンタの動作を図３のフローチャートにしたがって説明する。

【０２４０】

図３に示す通り、本実施例のセンタは、データの入力を待ち続け、入力があれば入力に応じた処理を行った後に再度入力待ちの状態に戻る終わる事のない処理である。

【０２４１】

最初に、入出力制御部２０１で入力があるかどうかがチェックされる（３０１）。ここで入力がなければ、再度入力のチェック（３０１）に戻る。

【０２４２】

入力のチェック（３０１）で入力があった場合、処理選択部２０２で、その入

力が検証用公開鍵情報依頼かどうかが判断される（３０２）。入力が検証用公開鍵情報依頼であれば、検証用公開鍵情報依頼処理部２０３が呼び出され検証用公開鍵情報依頼が処理される（３０３）。検証用公開鍵情報依頼の処理が終われば、再度入力のチェック（３０１）に戻る。

【０２４３】

３０２の判断で、入力が検証用公開鍵情報依頼でなければ、処理選択部２０２で、その入力が利用許可証依頼どうかが判断される（３０４）。入力が利用許可証依頼であれば、利用許可証依頼処理部２０４が呼び出され利用許可証依頼が処理される（３０５）。利用許可証依頼の処理が終われば、再度入力のチェック（３０１）に戻る。

【０２４４】

また、３０４の判断で、入力が利用許可証依頼でなければ、再度入力のチェック（３０１）に戻る。

【０２４５】

［検証用公開鍵情報依頼処理部］

図４は、本実施例のセンタが持つ検証用公開鍵情報依頼処理部２０３の内部構成を示した図である。

【０２４６】

検証用公開鍵情報依頼処理部２０３は、検証用公開鍵情報依頼を処理する機能を持ち、処理制御部４０１、署名検証部４０２、公開鍵ペア作成部４０３、公開鍵ペア識別子作成部４０４、検証用公開鍵情報作成部４０５、検証用公開鍵情報送付作成部４０６、エラーメッセージ作成部４０７、署名作成部４０８から構成される。

【０２４７】

検証用公開鍵情報依頼処理部２０３を構成する各部の役割を以下に述べる。

【０２４８】

処理制御部４０１：処理選択部２０２からの入力、入出力制御部２０１への出力、プロバイダＤＢ２０５の参照、公開鍵ペアＤＢ２０６へのエントリの追加の機能を担うとともに、検証用公開鍵情報依頼の処理全体を制御する。

署名検証部４０２：処理選択部２０２から入力される検証用公開鍵情報依頼のデジタル署名を検証する。

公開鍵ペア作成部４０３：検証用公開鍵および利用許可証の作成に使用される公開鍵ペアを作成する。

公開鍵ペア識別子作成部４０４：検証用公開鍵に割り当てられる検証用公開鍵識別子を作成する。十分に大きな空間からランダムにビット列を取り出す等、生成される識別子が重複しない工夫がなされている。

検証用公開鍵情報作成部４０５：検証用公開鍵情報を作成する。検証用公開鍵情報にデジタル署名を添付するために署名作成部４０８を呼び出す。

検証用公開鍵情報送付作成部４０６：検証用公開鍵情報送付を作成する。検証用公開鍵情報送付にデジタル署名を添付するために署名作成部４０８を呼び出す。さらに、センタの署名の検証鍵の公開鍵証明証を入手するために証明証記憶部２１１にアクセスする。

エラーメッセージ作成部４０７：エラーメッセージを作成する。

署名作成部４０８：検証用公開鍵情報、検証用公開鍵情報送付のためのデジタル署名を作成する。デジタル署名のための署名鍵を入手するために、署名鍵記憶部２１０にアクセスする。

【０２４９】

図５は、本実施例のセンタが持つ検証用公開鍵情報依頼処理部２０３の処理制御部４０１の動作を示すフローチャートである。処理制御部４０１の動作を図５にしたがって説明する。

【０２５０】

まず、処理選択部２０２から入力された検証用公開鍵情報依頼の公開鍵仕様フィールドに含まれる検証用公開鍵の使用者であるプロバイダの識別子を取り出し、センタがこの識別子のエンティティをプロバイダとして認めているかどうかをプロバイダＤＢ２０５を参照して調べる（５０１）。プロバイダＤＢ２０５にこの識別子を持つエントリが存在すれば、プロバイダとして認めたエンティティであることがわかる。

【０２５１】

５０１の判断で、プロバイダとして認めていないエンティティであることがわかった場合、エラーメッセージ作成部４０７でエラーメッセージを作成して入出力制御部２０１に出力した後（５０９）、終了する。

【０２５２】

５０１の判断で、プロバイダとして認めているエンティティであることがわかった場合、検証用公開鍵情報依頼のデジタル署名を検証する（５０２）。検証鍵は検証用公開鍵情報依頼の証明証フィールドに添付されているものを使用するが、必要な公開鍵証明証が証明証フィールドに存在しない場合には、ＣＡ１０８から公開鍵証明証を取得してから署名の検証を行う。

【０２５３】

署名の検証に失敗した場合、エラーメッセージ作成部４０７でエラーメッセージを作成して入出力制御部２０１に出力した後（５０９）、終了する。

【０２５４】

署名の検証に成功した場合、公開鍵ペア作成部４０３を呼び出してＲＳＡ公開鍵ペアを作成させ、作成された法数、公開鍵、秘密鍵を受け取る（５０３）。さらに、公開鍵ペア識別子作成部４０４を呼び出して検証用公開鍵情報に割り当てる識別子を作成させ、作成された識別子を受け取る（５０４）。

【０２５５】

次に検証用公開鍵情報の有効期間の開始日時と終了日時を適切に決定した後（５０５）、新しいエントリを公開鍵ペアＤＢに追加する（５０６）。新しいエントリの各属性には以下の値が設定される。

【０２５６】

【表２０】

公開鍵識別子属性：５０４で作成した識別子。

法数属性：５０３で作成したＲＳＡ法数。

公開鍵属性：５０３で作成したＲＳＡ公開鍵。

秘密鍵属性：５０３で作成したＲＳＡ秘密鍵。

プロバイダ識別子属性：検証用公開鍵情報依頼の公開鍵仕様フィールドに含まれる検証用公開鍵の使用者であるプロバイダの識別子。

有効期間開始属性：５０５で作成した有効期間の開始日時。

有効期間終了属性：５０５で作成した有効期間の終了日時。

発行日属性：現在の日時。

【０２５７】

次に、検証用公開鍵情報作成部（４０５）を呼び出し、検証用公開鍵情報を作成させ、その結果を受け取る（５０７）。検証用公開鍵情報の各フィールドには以下の値が設定される。

【０２５８】

【表２１】

発行者フィールド：自分自身すなわちセンタの識別子。

受領者フィールド：検証用公開鍵情報依頼の公開鍵仕様フィールドに含まれる検証用公開鍵の使用者であるプロバイダの識別子。

発行日フィールド：現在の時刻。

有効期間開始日時フィールド：５０５で作成した有効期間の開始日時。

有効期間終了日時フィールド：５０５で作成した有効期間の終了日時。

検証用公開鍵識別子フィールド：５０４で作成した識別子。

公開鍵情報フィールド：５０３で作成した法数、公開鍵、秘密鍵。

デジタル署名フィールド：このフィールド以外のフィールドのデータに対するデジタル署名。デジタル署名の作成のため、署名作成部４０８を呼び出し、結果の署名値を受け取り、このフィールドに設定する。

【０２５９】

最後に、検証用公開鍵情報送付作成部４０６を呼び出し、検証用公開鍵情報送付を作成させ、その結果を受け取って入出力制御部２０１に出力した後（５０８）、終了する。検証用公開鍵情報送付の各フィールドには以下の値が設定される。

【０２６０】

【表２２】

発信者フィールド：自分自身すなわちセンタの識別子。

受信者フィールド：検証用公開鍵情報依頼の発信者フィールドに記載されている

識別子。

日時フィールド：現在の時刻。

検証用公開鍵情報フィールド：５０７で作成した検証用公開鍵情報。

デジタル署名フィールド：このフィールドおよび証明証フィールド以外のフィールドのデータに対するデジタル署名。デジタル署名の作成のため、署名作成部４０８を呼び出し、結果の署名値を受け取り、このフィールドに設定する。

証明証フィールド：証明証記憶部２１１に記憶している公開鍵証明証。

【０２６１】

［利用許可証依頼処理部］

図１１は、本実施例のセンタが持つ利用許可証依頼処理部２０４の内部構成を示した図である。

【０２６２】

利用許可証依頼処理部２０４は、利用許可証依頼を処理する機能を持ち、処理制御部１１０１、署名検証部１１０２、仲介許諾内容確認部１１０３、利用許可証識別子作成部１１０４、利用許可証作成部１１０５、利用許可証送付作成部１１０６、エラーメッセージ作成部１１０７、署名作成部１１０８、証明値作成部１１０９、利用条件作成部１１１０から構成される。

【０２６３】

利用許可証依頼処理部２０４を構成する各部の役割を以下に述べる。

【０２６４】

処理制御部１１０１：処理選択部２０２からの入力、入出力制御部２０１への出力、公開鍵ペアＤＢ２０６リテーラＤＢ２０７消費者ＤＢ２０８の参照、利用許可証発行履歴ＤＢ２０９へのエントリの追加の機能を担うとともに、利用許可証依頼の処理全体を制御する。

署名検証部１１０２：処理選択部２０２から入力される利用許可証依頼、および該利用許可証依頼に含まれる仲介許諾証のデジタル署名を検証する。

仲介許諾内容確認部１１０３：処理選択部２０２から入力される利用許可証依頼で依頼された利用許可証の仲介が、該利用許可証依頼に含まれている仲介許諾証によって許諾されているかどうかを確認する。

利用許可証識別子作成部１１０４：利用許可証に割り当てられる利用許可証識別子を作成する。十分に大きな空間からランダムにビット列を取り出す等、生成される識別子が重複しない工夫がなされている。

利用許可証作成部１１０５：利用許可証を作成する。利用許可証にデジタル署名を添付するために署名作成部１１０８を呼び出す。

利用許可証送付作成部１１０６：利用許可証送付を作成する。利用許可証送付にデジタル署名を添付するために署名作成部１１０８を呼び出す。さらに、センタの署名の検証鍵の公開鍵証明証を入手するために証明証記憶部２１１にアクセスする。

エラーメッセージ作成部１１０７：エラーメッセージを作成する。

署名作成部１１０８：利用許可証、利用許可証送付のためのデジタル署名を作成する。デジタル署名のための署名鍵を入手するために、署名鍵記憶部２１０にアクセスする。

証明値作成部１１０９：利用許可証に含まれる証明値を作成する。

利用条件作成部１１１０：利用許可証に含まれる利用条件を作成する。

【０２６５】

図１２は、本実施例のセンタが持つ利用許可証依頼処理部２０４の処理制御部１１０１の動作を示すフローチャートである。処理制御部１１０１の動作を図１２にしたがって説明する。

【０２６６】

まず、処理選択部２０２から入力された利用許可証依頼の発信者フィールドに記載されている識別子を取り出し、センタがこの識別子のエンティティをリテーラとして認めているかどうかをリテーラＤＢ２０７を参照して調べる（１２０１）。リテーラＤＢ２０７にこの識別子を持つエントリが存在すれば、リテーラとして認めたエンティティであることがわかる。

【０２６７】

１２０１の判断で、リテーラとして認めていないエンティティであることがわかった場合、エラーメッセージ作成部１１０７でエラーメッセージを作成して入出力制御部２０１に出力した後（１２１０）、終了する。

【０２６８】

１２０１の判断で、リテーラとして認めているエンティティであることがわかった場合、利用許可証依頼のデジタル署名、および利用許可証依頼に含まれる仲介許諾証のデジタル署名を検証する（１２０２）。検証鍵は利用許可証依頼の証明証フィールドに添付されているものを使用するが、必要な公開鍵証明証が証明証フィールドに存在しない場合には、ＣＡ１０８から公開鍵証明証を取得してから署名の検証を行う。

【０２６９】

署名の検証に失敗した場合、エラーメッセージ作成部１１０７でエラーメッセージを作成して入出力制御部２０１に出力した後（１２１０）、終了する。

【０２７０】

署名の検証に成功した場合、利用許可証依頼で依頼された利用許可証の仲介が、該利用許可証依頼に含まれている仲介許諾証によって許諾されているかどうかを確認する（１２０３）。より具体的には、利用許可証依頼の許可内容フィールドに含まれている許可仕様を仲介許諾内容確認部１１０３に送付し、該許可仕様の公開鍵鍵識別子フィールドで指定されている検証用公開鍵識別子を持つ検証用公開鍵に対応する利用許可証を、該許可仕様の利用条件フィールドに記載されている利用条件で発行することが、該許可仕様の仲介許諾証フィールドに含まれている仲介許諾証で許諾されているかどうかを確認する。

【０２７１】

１２０３で、許諾されていない事がわかった場合、エラーメッセージ作成部１１０７でエラーメッセージを作成して入出力制御部２０１に出力した後（１２１０）、終了する。

【０２７２】

１２０３で、許諾されている事がわかった場合、利用許可証識別子作成部１１０４を呼び出して利用許可証に割り当てる識別子を作成させ、作成された識別子を受け取った後（１２０４）、利用条件作成部１１１０を呼び出して、利用許可証に記載する利用条件を決定する（１２０５）。利用条件作成部が生成する利用条件は、利用許可証依頼の許可内容フィールドに含まれている許可仕様の利用条

件フィールドの値そのままでもよいし、該許可仕様の仲介許諾証フィールドに含まれている仲介許諾証によって許諾されている範囲内で該利用条件フィールドの値を適切に修正したものであってもよい。

【０２７３】

利用条件の作成の後、新しいエントリを利用許可証発行履歴ＤＢ２０９に追加する（１２０６）。新しいエントリの各属性には以下の値が設定される。

【０２７４】

【表２３】

公開鍵識別子属性：利用許可証依頼の許可内容フィールドに含まれている許可仕様の公開鍵鍵識別子フィールドの値。

プロバイダ識別子属性：公開鍵ペアＤＢにアクセスし、該公開鍵ペアＤＢの公開鍵識別子属性が、利用許可証依頼の許可内容フィールドに含まれている許可仕様の公開鍵鍵識別子フィールドの値と同じ値を持つエントリの、プロバイダ識別子属性を取り出し、その値を設定する。

消費者識別子属性：利用許可証依頼の許可内容フィールドに含まれている許可仕様の消費者識別子フィールドの値。

仲介者識別子属性：利用許可証依頼の発信者フィールドの値。

利用条件属性：１２０５で利用条件作成部が作成した利用条件。

発行日属性：現在の日時。

【０２７５】

次に、証明値作成部１１０９を呼び出して証明値を作成させ、その結果を受け取る（１２０７）。さらに、利用許可証作成部１１０５を呼び出し、利用許可証を作成させ、その結果を受け取る（１２０８）。利用許可証の各フィールドには以下の値が設定される。

【０２７６】

【表２４】

発行者フィールド：自分自身すなわちセンタの識別子。

受領者フィールド：利用許可証依頼の許可内容フィールドに含まれている許可仕様の消費者識別子フィールドの値。

発行日フィールド：１２０６で利用許可証発行履歴ＤＢ２０９に追加したエントリの発行日属性の値。

利用許可証識別子フィールド：１２０４で作成した識別子。

公開鍵識別子フィールド：利用許可証依頼の許可内容フィールドに含まれている許可仕様の公開鍵鍵識別子フィールドの値。

利用条件フィールド：１２０５で利用条件作成部が作成した利用条件。

証明値フィールド：１２０７で作成した証明値。

デジタル署名フィールド：このフィールド以外のフィールドのデータに対するデジタル署名。デジタル署名の作成のため、署名作成部１１０８を呼び出し、結果の署名値を受け取り、このフィールドに設定する。

【０２７７】

最後に、利用許可証送付作成部１１０６を呼び出し、利用許可証送付を作成させ、その結果を受け取って入出力制御部２０１に出力した後（１２０９）、終了する。利用許可証送付の各フィールドには以下の値が設定される。

【０２７８】

【表２５】

発信者フィールド：自分自身すなわちセンタの識別子。

受信者フィールド：利用許可証依頼の発信者フィールドの値。

日時フィールド：現在の時刻。

利用許可証フィールド：１２０８で作成した利用許可証。

デジタル署名フィールド：このフィールドおよび証明証フィールド以外のフィールドのデータに対するデジタル署名。デジタル署名の作成のため、署名作成部１１０８を呼び出し、結果の署名値を受け取り、このフィールドに設定する。

証明証フィールド：証明証記憶部２１１に記憶している公開鍵証明証。

【０２７９】

［センタが持つその他の機能］

本実施例のセンタは、利用許可証発行の履歴情報をプロバイダに送付する事ができる。

【０２８０】

プロバイダに渡される利用許可証発行の履歴情報は、そのプロバイダに割り当てられた検証用公開鍵に対応する利用許可証の発行についての情報であり、利用許可証発行プロバイダ用履歴作成部２１２で作成され、入出力制御部２０１を介してプロバイダに送付される。プロバイダにとっては、この履歴情報は、自己が提供しているデジタルコンテンツをどのリテーラがどのぐらい販売したかのを示す信頼できる情報であり、販売におけるマージンがリテーラからプロバイダに渡される場合に、リテーラから送られたマージンの正しさをプロバイダが確認する際の重要な情報となる。

【０２８１】

利用許可証発行プロバイダ用履歴作成部２１２は、履歴を作成するプロバイダの識別子と履歴作成の対象期間の開始日時と終了日時の指定を受け、利用許可証発行履歴ＤＢ２０９から、プロバイダ識別子属性の値が指定されたプロバイダの識別子と一致し、発行日属性の値が指定された履歴作成の対象期間内であるエントリ群を取り出し、その公開鍵識別子属性、仲介者識別子属性、利用条件属性、発行日属性の値を取り出す。本実施例では、履歴を作成するプロバイダの識別子と履歴作成の対象期間の指定はセンタのオペレータから受けるが、インターネット経由でプロバイダから入力されるように構成してもよい。

【０２８２】

本実施例のセンタは、利用許可証発行の履歴情報をリテーラにも送付する事ができる。

【０２８３】

リテーラに渡される利用許可証発行の履歴情報は、そのリテーラからの依頼で行った利用許可証の発行についての情報であり、利用許可証発行リテーラ用履歴作成部２１３で作成され、入出力制御部２０１を介してリテーラに送付される。この履歴は、センタがリテーラから利用許可証発行のマージンを受け取る場合のマージンの額の根拠となる。

【０２８４】

利用許可証発行リテーラ用履歴作成部２１３は、履歴を作成するリテーラの識別子と履歴作成の対象期間の開始日時と終了日時の指定を受け、利用許可証発行

履歴ＤＢ２０９から、仲介者識別子属性の値が指定されたリテーラの識別子と一致し、発行日属性の値が指定された履歴作成の対象期間内であるエントリ群を取り出し、その公開鍵識別子属性、プロバイダ識別子属性、消費者識別子属性、利用条件属性、発行日属性の値を取り出す。本実施例では、履歴を作成するリテーラの識別子と履歴作成の対象期間の指定はセンタのオペレータから受けるが、インターネット経由でリテーラから入力されるように構成してもよい。

【０２８５】

また、本実施例のセンタは、検証用公開鍵情報発行の履歴情報をプロバイダに送付する事ができる。

【０２８６】

プロバイダに渡される検証用公開鍵情報発行の履歴情報は、そのプロバイダに対して発行された検証用公開鍵情報についての情報であり、検証用公開鍵情報発行履歴作成部２１４で作成され、入出力制御部２０１を介してプロバイダに送付される。この履歴は、センタがプロバイダから検証用公開鍵情報発行の手数料を徴収する場合の根拠となる。

【０２８７】

検証用公開鍵情報発行履歴作成部２１４は、履歴を作成するプロバイダの識別子と履歴作成の対象期間の開始日時と終了日時の指定を受け、履歴を作成するプロバイダの識別子と履歴作成の対象期間の開始日時と終了日時の指定を受け、公開鍵ペアＤＢ２０６から、公開鍵識別子属性、法数属性、公開鍵属性、有効期間開始属性、有効期間終了属性、発行日属性の値を取り出す。本実施例では、履歴を作成するプロバイダの識別子と履歴作成の対象期間の指定はセンタのオペレータから受けるが、インターネット経由でプロバイダから入力されるように構成してもよい。

【０２８８】

上記の履歴情報のプロバイダやリテーラへの送付方法は、電子メールでもよいし、ＷＷＷベースでオンデマンドで発行してもよい。盗聴や改竄の危険がある場合は暗号化やデジタル署名が適用されるのが望ましい。

【０２８９】

［プロバイダの構成］

図１３は、本実施例のプロバイダの構成図である。

【０２９０】

本実施例のプロバイダは、検証用公開鍵情報依頼を作成してインターネットを介してセンタに送付する機能と、インターネットを介して入力される検証用公開鍵情報送付と仲介許諾証依頼とを処理する機能を持つ。プロバイダは、入出力制御部１３０１、処理選択部１３０２、検証用公開鍵情報依頼作成部１３０３、検証用公開鍵情報送付処理部１３０４、仲介許諾証依頼処理部１３０５、検証用公開鍵ＤＢ１３０６、署名鍵記憶部１３０７、証明証記憶部１３０８、仲介許諾証発行履歴ＤＢ１３０９、仲介許諾証発行履歴作成部１３１０から構成され、入出力制御部１３０１を介してインターネットに接続されている。

【０２９１】

本実施例のプロバイダの各部の役割を以下に述べる。

【０２９２】

入出力制御部１３０１：インターネットを介したデータの入力を監視するとともに、検証用公開鍵情報依頼作成部１３０３や仲介許諾証依頼処理部１３０５が作成したデータをインターネットを介して出力する。インターネットからの入出力制御部１３０１への入力、あるいは、入出力制御部１３０１からインターネットへの出力の方法としては、入出力制御部１３０１と接続されたＷＷＷサイトを準備して他のエンティティにアクセスさせるもの、他のエンティティが用意しているＷＷＷサイトにアクセスしてプロバイダが作成したデータを送るもの、あるいは電子メールシステムと入出力制御部１３０１を自動的にあるいは人手によって連動させるものなどが使用できる。

処理選択部１３０２：入力したデータが検証用公開鍵情報送付かまたは仲介許諾証依頼かを判断し、検証用公開鍵情報送付であれば検証用公開鍵情報送付処理部１３０４を、仲介許諾証依頼であれば仲介許諾証依頼処理部１３０５を呼び出す。

検証用公開鍵情報依頼作成部１３０３：検証用公開鍵情報依頼を作成し、入出力制御部１３０１を介してセンタに送付する。検証用公開鍵情報依頼作成の過程で

、署名鍵記憶部１３０７と証明証記憶部１３０８にアクセスする。

検証用公開鍵情報送付処理部１３０４：検証用公開鍵情報送付を処理し、検証用公開鍵を検証用公開鍵ＤＢ１３０６に登録する。

仲介許諾証依頼処理部１３０５：仲介許諾証依頼を処理し、仲介許諾証送付を作成して入出力制御部１３０１を介して依頼者に送付する。仲介許諾証送付作成の過程で検証用公開鍵ＤＢ１３０６を参照するとともに、仲介許諾発行履歴ＤＢ１３０９に新しいエントリを追加し、署名鍵記憶部１３０７と証明証記憶部１３０８にアクセスする。

検証用公開鍵ＤＢ１３０６：検証用公開鍵に関する情報を保持するＤＢ。

署名鍵記憶部１３０７：プロバイダが作成するデジタル署名に使用する署名鍵を保持する。

証明証記憶部１３０８：署名鍵記憶部１３０７に記憶されている署名鍵で作成したデジタル署名を検証できる検証鍵を含む公開鍵証明証を保持する。

仲介許諾証発行履歴ＤＢ１３０９：仲介許諾証の発行の履歴を保持するＤＢ。

仲介許諾証発行履歴作成部１３１０：リテーラ毎の仲介許諾証の発行履歴を作成する。

【０２９３】

［プロバイダが持つデータベース］

プロバイダは、検証用公開鍵ＤＢ１３０６、仲介許諾証発行履歴ＤＢ１３０９の２つのデータベースを持っている。

【０２９４】

検証用公開鍵ＤＢ１３０６は、センタから発行を受けた検証用公開鍵情報の内容を、プロバイダ自身が決定した検証用公開鍵の用途とともに保持するデータベースである。

【０２９５】

検証用公開鍵ＤＢ１３０６の構造を図１４に示す。検証用公開鍵ＤＢ１３０６は以下の６つの属性からなるテーブルであり、各エントリはそれぞれ一つの検証用公開鍵に関する情報である。

【０２９６】

【表２６】

公開鍵識別子属性：検証用公開鍵に割り当てられた検証用公開鍵識別子。

法数属性：検証用公開鍵情報に含まれていたＲＳＡ法数。

公開鍵属性：検証用公開鍵情報に含まれていたＲＳＡ公開鍵。

有効期間開始属性：検証用公開鍵情報の有効期間の開始日時。

有効期間終了属性：検証用公開鍵情報の有効期間の終了日時。

用途属性：このエントリの検証用公開鍵に対してプロバイダが割り当てた用途。この検証用公開鍵で利用許可証の正当性を検証するデジタルコンテンツあるいはその機能の情報である。

【０２９７】

仲介許諾証発行履歴ＤＢ１３０９は、プロバイダが発行した仲介許諾証に関する履歴を保持するデータベースである。

【０２９８】

仲介許諾証発行履歴ＤＢ１３０９の構造を図３４に示す。仲介許諾証発行履歴ＤＢ１３０９は以下の７つの属性からなるテーブルであり、各エントリはそれぞれ一回の仲介許諾証の発行に関する情報である。

【０２９９】

【表２７】

仲介許諾証識別子属性：発行した仲介許諾証に割り当てられた識別子。

公開鍵識別子属性：発行した仲介許諾証で利用許可証の仲介が許諾される検証用公開鍵に割り当てられた検証用公開鍵識別子。

リテーラ識別子属性：発行した仲介許諾証で許諾をうけるリテーラの識別子。

利用条件限定情報属性：発行した仲介許諾証に記載されている利用条件限定情報。有効期間開始属性：発行した仲介許諾証の有効期間の開始日時。

有効期間終了属性：発行した仲介許諾証の有効期間の終了日時。

発行日属性：発行した仲介許諾証の発行日時。

【０３００】

［検証用公開鍵情報依頼作成部］

本実施例のプロバイダは、新たに販売を開始したいデジタルコンテンツが発生

した時に、そのデジタルコンテンツに割り当てる検証用公開鍵を含む検証用公開鍵情報の発行をセンタに依頼する。依頼の際には、検証用公開鍵情報依頼作成部１３０３において検証用公開鍵情報依頼を作成し、入出力制御部１３０１を介してセンタに送付する。

【０３０１】

検証用公開鍵情報依頼作成部１３０３では、検証用公開鍵情報依頼の各フィールドに以下の値を設定する。

【０３０２】

【表２８】

発信者フィールド：自分自身すなわちプロバイダの識別子。

受信者フィールド：センタの識別子。

日時フィールド：現在の時刻。

公開鍵仕様フィールド：作成してもらう検証用公開鍵に対する要望。検証用公開鍵の使用者として自分の識別子を記載し、さらに、要望する公開鍵暗号アルゴリズムと鍵長が記載される。本実施例では公開鍵暗号アルゴリズムとしてはＲＳＡのみが使用可能なので、公開鍵暗号アルゴリズムの値はＲＳＡで固定である。

デジタル署名フィールド：このフィールドおよび証明証フィールド以外のフィールドのデータに対するデジタル署名。デジタル署名の作成のため、検証用公開鍵情報依頼作成部１３０３は署名作成部を含んでおり、この署名作成部が作成した署名値をこのフィールドに設定する。署名鍵は署名鍵記憶部１３０７にアクセスして入手する。

証明証フィールド：証明証記憶部１３０８に記憶している公開鍵証明証。

【０３０３】

［検証用公開鍵情報送付処理部］

検証用公開鍵情報依頼作成部１３０３で検証用公開鍵情報依頼が作成されセンタに送付されると、その返信としてセンタから検証用公開鍵情報送付が送信されてくる。検証用公開鍵情報送付は、入出力制御部１３０１および処理選択部１３０２を経由して検証用公開鍵情報送付処理部１３０４へ送られ、そこで処理される。

【０３０４】

図１５は、本実施例のプロバイダが持つ検証用公開鍵情報送付処理部１３０４の動作を示すフローチャートである。検証用公開鍵情報送付処理部１３０４の動作を図１５にしたがって説明する。

【０３０５】

まず、処理選択部１３０２から入力された検証用公開鍵情報送付、および、該検証用公開鍵情報送付に含まれる検証用公開鍵情報のデジタル署名を検証する（１５０１）。検証鍵は検証用公開鍵情報送付の証明証フィールドに添付されているものを使用するが、必要な公開鍵証明証が証明証フィールドに存在しない場合には、ＣＡ１０８から公開鍵証明証を取得してから署名の検証を行う。署名の検証のために、検証用公開鍵情報送付処理部１３０４はデジタル署名の検証を専門に行う署名検証部を含んでいる。

【０３０６】

１５０１で、デジタル署名の検証に失敗した場合、エラー処理を行った後（１５０５）、終了する。

【０３０７】

１５０１で、デジタル署名の検証に成功した場合、検証用公開鍵情報送付に含まれている検証用公開鍵情報の発行者がセンタであるかどうかが調べられる（１５０２）。この検査は、検証用公開鍵情報の発行者フィールドに記載されている識別子がセンタのものであるかどうかで検査できる。

【０３０８】

１５０２の検査で、検証用公開鍵情報の発行者がセンタでなかった場合、エラー処理を行った後（１５０５）、終了する。

【０３０９】

１５０２の検査で、検証用公開鍵情報の発行者がセンタであったら、次に検証用公開鍵ＤＢ１３０６に新しいエントリを追加する（１５０３）。新しいエントリの各属性には以下の値が設定される。

【０３１０】

【表２９】

公開鍵識別子属性：検証用公開鍵情報送付に含まれている検証用公開鍵情報の検証用公開鍵識別子フィールドの値。

法数属性：検証用公開鍵情報送付に含まれている検証用公開鍵情報の、公開鍵情報フィールドに含まれていたＲＳＡ法数。

公開鍵属性：検証用公開鍵情報送付に含まれている検証用公開鍵情報の、公開鍵情報フィールドに含まれていたＲＳＡ公開鍵。

有効期間開始属性：検証用公開鍵情報送付に含まれている検証用公開鍵情報の有効期間開始日時フィールドの値。

有効期間終了属性：検証用公開鍵情報送付に含まれている検証用公開鍵情報の有効期間終了日時フィールドの値。

用途属性：この検証用公開鍵にプロバイダ割り当てた用途についての情報。

【０３１１】

［仲介許諾依証頼処理部］

図１６は、本実施例のプロバイダが持つ仲介許諾証依頼処理部１３０５の内部構成を示した図である。

【０３１２】

仲介許諾証依頼処理部１３０５は、仲介許諾証依頼を処理する機能を持ち、処理制御部１６０１、署名検証部１６０２、仲介許諾証識別子作成部１６０３、エラーメッセージ作成部１６０４、仲介許諾証作成部１６０５、仲介許諾証送付作成部１６０６、署名作成部１６０７、利用条件限定情報作成部１６０８から構成される。

【０３１３】

仲介許諾証依頼処理部１３０５を構成する各部の役割を以下に述べる。

【０３１４】

処理制御部１６０１：処理選択部１３０２からの入力、入出力制御部１３０１への出力、検証用公開鍵ＤＢ１３０６の参照、仲介許諾証発行履歴ＤＢ１３０９へのエントリの追加の機能を担うとともに、仲介許諾証依頼の処理全体を制御する。

署名検証部１６０２：処理選択部２０２から入力される仲介許諾証依頼のデジタ

ル署名を検証する。

仲介許諾証識別子作成部１６０３：仲介許諾証に割り当てられる仲介許諾証識別子を作成する。十分に大きな空間からランダムにビット列を取り出す等、生成される識別子が重複しない工夫がなされている。

エラーメッセージ作成部１６０４：エラーメッセージを作成する。

仲介許諾証作成部１６０５：仲介許諾証を作成する。仲介許諾証にデジタル署名を添付するために署名作成部１６０７を呼び出す。

仲介許諾証送付作成部１６０６：仲介許諾証送付を作成する。仲介許諾証送付にデジタル署名を添付するために署名作成部１６０７を呼び出す。さらに、プロバイダの署名の検証鍵の公開鍵証明証を入手するために証明証記憶部１３０８にアクセスする。

署名作成部１６０７：仲介許諾証、仲介許諾証送付のためのデジタル署名を作成する。デジタル署名のための署名鍵を入手するために、署名鍵記憶部１３０７にアクセスする。

利用条件限定情報作成部１６０８：仲介許諾証に記載される利用条件限定情報を作成する。

【０３１５】

図１７は、本実施例のプロバイダが持つ仲介許諾証依頼処理部１３０５の処理制御部１６０１の動作を示すフローチャートである。処理制御部１６０１の動作を図１７にしたがって説明する。

【０３１６】

まず、処理選択部１３０２から入力された仲介許諾証依頼のデジタル署名を検証する（１７０１）。検証鍵は仲介許諾証依頼の証明証フィールドに添付されているものを使用するが、必要な公開鍵証明証が証明証フィールドに存在しない場合には、ＣＡ１０８から公開鍵証明証を取得してから署名の検証を行う。

【０３１７】

署名の検証に失敗した場合、エラーメッセージ作成部１６０４でエラーメッセージを作成して入出力制御部１３０１に出力した後（１７０９）、終了する。

【０３１８】

署名の検証に成功した場合、仲介許諾証依頼で依頼された仲介許諾証を発行するかどうかを決定する（１７０２）。仲介許諾証を発行するかどうかの決定はプロバイダにまかされている。例えば、仲介許諾証によって許諾を受けるリテーラを信用できない場合や、仲介許諾証依頼に含まれる仲介許諾証仕様の許諾者フィールドに記載されている識別子が自分のものと異なる場合や、仲介許諾証依頼に含まれる仲介許諾仕様の公開鍵鍵識別子フィールドに記載された検証用公開鍵識別子を持つ検証用公開鍵情報が自分に対して発行されたものでない場合や、仲介許諾証依頼に含まれる仲介許諾仕様の希望利用条件限定情報フィールドの希望にそえない場合に仲介許諾証の発行をやめることになる。

【０３１９】

１７０２で、仲介許諾証を発行しないと決定した場合には、エラーメッセージ作成部１６０４でエラーメッセージを作成して入出力制御部１３０１に出力した後（１７０９）、終了する。

【０３２０】

１７０２で、仲介許諾証を発行すると決定した場合には、仲介許諾証識別子作成部１６０３を呼び出して仲介許諾証に割り当てる識別子を作成させ、作成された識別子を受け取った後（１７０３）、発行する仲介許諾証の有効期間を適切に決定する（１７０４）。

【０３２１】

さらに、利用条件限定情報作成部１６０８を呼び出して発行する仲介許諾証に含まれる利用条件限定情報を作成させ、その結果を受け取る（１７０５）。ここで作成する利用条件限定情報は、仲介許諾証依頼に含まれる仲介許諾仕様の希望利用条件限定情報フィールドに記載されいるものでもよいし、プロバイダが自己の判断で適切な利用条件限定情報を決定してもよい。

【０３２２】

その後、仲介許諾証作成部１６０５を呼び出し、仲介許諾証を作成させ、その結果を受け取る（１７０６）。仲介許諾証の各フィールドには以下の値が設定される。

【０３２３】

【表３０】

発行者フィールド：自分自身すなわちプロバイダの識別子。

受領者フィールド：仲介許諾証依頼に含まれる仲介許諾仕様の被許諾者フィールドの値。

発行日フィールド：現在の日時。

仲介許諾証識別子フィールド：１７０３で作成した識別子。

有効期間開始日時フィールド：１７０４で決定した有効期間の開始日時。

有効期間終了日時フィールド：１７０４で決定した有効期間の終了日時。

公開鍵鍵識別子フィールド：仲介許諾証依頼に含まれる仲介許諾仕様の公開鍵鍵識別子フィールドの値。

利用条件限定情報フィールド：１７０５で決定した利用条件限定情報の値。

デジタル署名フィールド：このフィールド以外のフィールドのデータに対するデジタル署名。デジタル署名の作成のため、署名作成部１６０７を呼び出し、結果の署名値を受け取り、このフィールドに設定する。

【０３２４】

次に、仲介許諾証送付作成部１６０６を呼び出し、仲介許諾証送付を作成させ、その結果を受け取って入出力制御部１３０１に出力する（１７０７）。仲介許諾証送付の各フィールドには以下の値が設定される。

【０３２５】

【表３１】

発信者フィールド：自分自身すなわちプロバイダの識別子。

受信者フィールド：仲介許諾証依頼の発信者フィールドに記載されている識別子。

日時フィールド：現在の日時。

仲介許諾証フィールド：１７０６で作成した仲介許諾証。

デジタル署名フィールド：このフィールドおよび証明証フィールド以外のフィールドのデータに対するデジタル署名。デジタル署名の作成のため、署名作成部１６０７を呼び出し、結果の署名値をこのフィールドに設定する。

【０３２６】

【表３２】

証明証フィールド：証明証記憶部１３０８に記憶している公開鍵証明証。

【０３２７】

最後に仲介許諾証発行の履歴を表す新しいエントリを仲介許諾証発行履歴ＤＢ１３０９に追加して終了する。追加されるエントリの各属性には以下の値が格納される。

【０３２８】

【表３３】

仲介許諾証識別子属性：１７０３で作成した識別子。

公開鍵識別子属性：仲介許諾証依頼に含まれる仲介許諾仕様の公開鍵識別子フィールドの値。

リテーラ識別子属性：仲介許諾証依頼に含まれる仲介許諾仕様の被許諾者フィールドの値。

利用条件限定情報属性：１７０５で決定した利用条件限定情報の値。

有効期間開始属性：１７０４で決定した有効期間の開始日時。

有効期間終了属性：１７０４で決定した有効期間の終了日時。

発行日属性：１７０５で作成した仲介許諾証の発行日フィールドに記載した値。

【０３２９】

［プロバイダが持つその他の機能］

本実施例のプロバイダは、仲介許諾証発行の履歴情報をリテーラに送付する事ができる。

【０３３０】

リテーラに渡される仲介許諾証発行の履歴情報は、そのリテーラに発行された仲介許諾証についての情報であり、仲介許諾証発行履歴作成部１３１０で作成され、入出力制御部１３０１を介してリテーラに送付される。この履歴は、プロバイダがリテーラに対して仲介許諾証発行の手数料を請求する場合の根拠となる。

【０３３１】

仲介許諾証発行履歴作成部１３１０は、履歴を作成するリテーラの識別子と履歴作成の対象期間の開始日時と終了日時の指定を受け、仲介許諾証発行履歴ＤＢ

１３０９から、リテーラ識別子属性の値が指定されたリテーラの識別子と一致し、発行日属性の値が指定された履歴作成の対象期間内であるエントリ群を取り出し、その仲介許諾証識別子属性、公開鍵識別子属性、利用条件限定情報属性、有効期間開始属性、有効期間終了属性、発行日属性の値を取り出す。本実施例では、履歴を作成するリテーラの識別子と履歴作成の対象期間の指定はプロバイダのオペレータから受けるが、インターネット経由でリテーラから入力されるように構成してもよい。

【０３３２】

上記の履歴情報の送付方法は、電子メールでもよいし、ＷＷＷベースでオンデマンドで発行してもよい。盗聴や改竄の危険がある場合は暗号化やデジタル署名が適用されるのが望ましい。

【０３３３】

［リテーラの構成］

図１８は、本実施例のリテーラの構成図である。

【０３３４】

本実施例のリテーラは、仲介許諾証依頼を作成してインターネットを介してプロバイダに送付する機能、インターネットを介して入力される仲介許諾証送付、利用許可証依頼、利用許可証送付を処理する機能、利用許可証仲介の履歴を作成してインターネットを介してプロバイダや利用許可証仲介の依頼者に送付する機能を持つ。リテーラは、入出力制御部１８０１、処理選択部１８０２、仲介許諾証依頼作成部１８０３、利用許可証依頼処理部１８０４、仲介許諾証送付処理部１８０５、利用許可証送付処理部１８０６、仲介許諾証ＤＢ１８０７、利用許可証仲介履歴ＤＢ１８０８、署名鍵記憶部１８０９、証明証記憶部１８１０、利用許可証仲介プロバイダ用履歴作成部１８１１、利用許可証仲介依頼者用履歴作成部１８１２から構成され、入出力制御部１８０１を介してインターネットに接続されている。

【０３３５】

本実施例のリテーラの各部の役割を以下に述べる。

【０３３６】

入出力制御部１８０１：インターネットを介したデータの入力を監視するとともに、仲介許諾証依頼作成部１８０３、利用許可証依頼処理部１８０４、利用許可証送付処理部１８０６が作成したデータをインターネットを介して出力する。インターネットからの入出力制御部１８０１への入力、あるいは、入出力制御部１８０４からインターネットへの出力の方法としては、入出力制御部１８０１と接続されたWWWサイトを準備して他のエンティティにアクセスさせるもの、他のエンティティが用意しているWWWサイトにアクセスしてリテーラが作成したデータを送るもの、あるいは電子メールシステムと入出力制御部１８０１を自動的にあるいは人手によって連動させるものなどが使用できる。

処理選択部１８０２：入力したデータが、利用許可証依頼、仲介許諾証送付、利用許可証送付のいずれであるかを判断し、利用許可証依頼であれば利用許可証依頼処理部１８０４を、仲介許諾証送付であれば仲介許諾証送付処理部１８０５を、利用許可証送付であれば利用許可証送付処理部１８０６を呼び出す。

仲介許諾証依頼作成部１８０３：仲介許諾証依頼を作成し、入出力制御部１８０１を介してプロバイダに送付する。仲介許諾証依頼作成の過程で、署名鍵記憶部１８０９と証明証記憶部１８１０にアクセスする。

利用許可証依頼処理部１８０４：消費者からの利用許可証依頼を処理し、第二の利用許可証依頼を作成して、入出力制御部１８０１を介してセンタに送付する。処理の過程で、仲介許諾証ＤＢ１８０７を参照するとともに、署名鍵記憶部１８０９と証明証記憶部１８１０にアクセスする。

仲介許諾証送付処理部１８０５：プロバイダからの仲介許諾証送付を処理し、該仲介許諾証送付に含まれている仲介許諾証を仲介許諾証ＤＢ１８０７に登録する。

利用許可証送付処理部１８０６：センタからの利用許可証送付を処理し、第二の利用許可証送付をを作成して、入出力制御部１８０１を介して利用許可証の依頼者に送付する。処理の過程で、利用許可証仲介履歴ＤＢ１８０８を更新するとともに、署名鍵記憶部１８０９と証明証記憶部１８１０にアクセスする。

仲介許諾証ＤＢ１８０７：プロバイダからこのリテーラに対して発行された仲介許諾証に関する情報を保持するＤＢ。

利用許可証仲介履歴ＤＢ１８０８：このリテーラが仲介した利用許可証についての履歴を保持するＤＢ。

署名鍵記憶部１８０９：リテーラが作成するデジタル署名に使用する署名鍵を保持する。

証明証記憶部１８１０：署名鍵記憶部１８０９に記憶されている署名鍵で作成したデジタル署名を検証できる検証鍵を含む公開鍵証明証を保持する。

利用許可証仲介プロバイダ用履歴作成部１８１１：各プロバイダ毎の利用許可証仲介の履歴を作成し、入出力制御部１８０１を介してプロバイダに送付する。

利用許可証仲介依頼者用履歴作成部１８１２：リテーラが受け取った利用許可証仲介依頼の依頼者毎の利用許可証仲介の履歴を作成し、入出力制御部１８０１を介して依頼者に送付する。

【０３３７】

[リテーラが持つデータベース]

リテーラは、仲介許諾証ＤＢ１８０７と利用許可証仲介履歴ＤＢ１８０８の２つのデータベースを持っている。

【０３３８】

仲介許諾証ＤＢ１８０７は、リテーラが複数のプロバイダから受けた仲介許諾証に関する情報を保持したデータベースである。

【０３３９】

仲介許諾証ＤＢ１８０７の構造を図１９に示す。仲介許諾ＤＢ１８０７は以下の５つの属性からなるテーブルである。各エントリがそれぞれ一つの仲介許諾証にあたる。

【０３４０】

【表３４】

仲介許諾証識別子属性：プロバイダから発行された仲介許諾証に割り当てられている仲介許諾証識別子。

公開鍵識別子属性：プロバイダから発行された仲介許諾証で利用許可証発行の仲介が許諾された検証用公開鍵の識別子。

プロバイダ識別子属性：仲介許諾証を発行したプロバイダの識別子。

仲介許諾証属性：プロバイダから発行された仲介許諾証自体をＢＥＲにしたがってエンコードしたデータ。

プロバイダ証明証属性：仲介許諾証を発行したプロバイダのデジタル署名を検証できる公開鍵を含む公開鍵証明証をＢＥＲにしたがってエンコードしたデータ。

【０３４１】

利用許可証仲介履歴ＤＢ１８０８は、リテーラが仲介した利用許可証に関する情報を保持したデータベースである。

【０３４２】

利用許可証仲介履歴ＤＢ１８０８の構造を図２０に示す。利用許可証仲介履歴ＤＢ１８０８は以下の８つの属性からなるテーブルである。各エントリがそれぞれ一つの利用許可証の仲介にあたる。

【０３４３】

【表３５】

利用許可証識別子属性：仲介した利用許可証にセンタが割り当てた識別子。

公開鍵識別子属性：仲介した利用許可証の正当性を検証できる検証用公開鍵にセンタが割り当てた識別子。

プロバイダ識別子属性：公開鍵識別子属性で指定された検証用公開鍵のユーザであるプロバイダの識別子。

消費者識別子属性：利用許可証の発行を受けた消費者の識別子。

依頼者識別子属性：利用許可証依頼をリテーラに送付してきたエンティティの識別子。

利用条件属性：仲介された利用許可証に記載された利用条件。

依頼日時属性：リテーラが受け取った利用許可証依頼の作成日時。

発信日時属性：リテーラが利用許可証送付を作成した日時。

【０３４４】

［仲介許諾証依頼作成部］

本実施例のリテーラは、プロバイダが提供しているデジタルコンテンツの販売を始めたい場合、そのデジタルコンテンツに割りあてられた検証用公開鍵に対応する利用許可証の仲介を許諾する仲介許諾証をプロバイダから受けなければなら

ない。プロバイダから仲介許諾証を受け取るため、リテーラは仲介許諾証依頼作成部１８０３において仲介許諾証依頼を作成し、入出力制御部１８０１を介してプロバイダに送付する。

【０３４５】

仲介許諾証依頼作成部１８０３では、仲介許諾証依頼の各フィールドに以下の値を設定する。

【０３４６】

【表３６】

発信者フィールド：自分自身すなわちリテーラの識別子。

受信者フィールド：仲介許諾証の依頼先であるプロバイダの識別子。

日時フィールド：現在の時刻。

仲介許諾仕様フィールド：作成してもらう仲介許諾証に対するリテーラからの希望を記載する。

デジタル署名フィールド：このフィールドおよび証明証フィールド以外のフィールドのデータに対するデジタル署名。デジタル署名の作成のため、仲介許諾証依頼作成部１８０３は署名作成部を含んでおり、この署名作成部が作成した署名値をこのフィールドに設定する。署名鍵は署名鍵記憶部１８０９にアクセスして入手する。

証明証フィールド：証明証記憶部１８１０に記憶している公開鍵証明証。

【０３４７】

仲介許諾証依頼の仲介許諾仕様フィールドに記載される仲介許諾仕様の各フィールドには以下の値が設定される。

【０３４８】

【表３７】

許諾者フィールド：仲介許諾証を発行してほしいプロバイダの識別子。

被許諾者フィールド：自分自身すなわちリテーラの識別子。

公開鍵識別子フィールド：仲介許諾証を発行してほしい検証用公開鍵に割り当てられた検証用公開鍵識別子。

希望利用条件限定情報フィールド：リテーラが仲介許諾証に記載してほしいと希

望する利用条件限定情報。

【０３４９】

［仲介許諾証送付処理部］

仲介許諾依頼作成部１８０３で仲介許諾証依頼が作成されプロバイダに送付されると、その返信としてプロバイダから仲介許諾証送付が送信されてくる。仲介許諾証送付は、入出力制御部１８０１および処理選択部１８０２を経由して仲介許諾証送付処理部１８０５に送られ、そこで処理される。

【０３５０】

図２１は、本実施例のリテーラが持つ仲介許諾証送付処理部１８０５の動作を示すフローチャートである。仲介許諾証送付処理部１８０５の動作を図２１にしたがって説明する。

【０３５１】

まず、処理選択部１８０２から入力された仲介許諾証送付、および、該仲介許諾証送付に含まれる仲介許諾証のデジタル署名を検証する（２１０１）。検証鍵は仲介許諾証送付の証明証フィールドに添付されているものを使用するが、必要な公開鍵証明証が証明証フィールドに存在しない場合には、ＣＡ１０８から公開鍵証明証を取得してから署名の検証を行う。署名の検証のために、仲介許諾証送付処理部１８０５はデジタル署名の検証を専門に行う署名検証部を含んでいる。

【０３５２】

２１０１で、デジタル署名の検証に失敗した場合、エラー処理を行った後（２１０４）、終了する。

【０３５３】

２１０１で、デジタル署名の検証に成功した場合、仲介許諾証送付に含まれている仲介許諾証の作成者が正しいプロバイダであるかどうかが確認される（２１０２）。正しいプロバイダであるかどうかの判断基準にはいくつかバリエーションが有り得る。たとえば、仲介許諾証送付に含まれている仲介許諾証の発行者フィールドの値が、自分が依頼した仲介許諾証依頼に含まれる仲介許諾仕様の許諾者フィールドに記載されている識別子と一致するという基準はその一例である。仲介許諾証送付に含まれている仲介許諾証で利用許可証の仲介が許諾される検証

用公開鍵と、該仲介許諾証の発行者との関係を確認したければ、センタが発行した検証用公開鍵情報を確認すればよい。検証用公開鍵情報は公開可能な情報であるので、センタあるいはプロバイダが検証用公開鍵情報を自由にダウンロードできる形で公開することが可能である。

【０３５４】

２１０２の検査で、仲介許諾証の作成者が正しいプロバイダではなかった場合、エラー処理を行った後（２１０４）、終了する。

【０３５５】

２１０２の検査で、仲介許諾証の作成者が正しいプロバイダと判断した場合、仲介許諾証ＤＢ１８０７に新しいエントリを追加する（２１０３）。新しいエントリの各属性には以下の値が設定される。

【０３５６】

【表３８】

仲介許諾証識別子属性：仲介許諾証送付に含まれる仲介許諾証の仲介許諾証識別子フィールドの値。

公開鍵識別子属性：仲介許諾証送付に含まれる仲介許諾証の公開鍵鍵識別子フィールドの値。

プロバイダ識別子属性：仲介許諾証送付に含まれる仲介許諾証の発行者フィールドの値。

仲介許諾証属性：　仲介許諾証送付に含まれる仲介許諾証をＢＥＲにしたがってエンコードした結果。

プロバイダ証明証属性：仲介許諾証送付に含まれるプロバイダの署名の検証鍵を含む公開鍵証明証をＢＥＲにしたがってエンコードした結果。

【０３５７】

［利用許可証依頼処理部］

図２２は、本実施例のリテーラが持つ利用許可証依頼処理部１８０４の内部構成を示した図である。

【０３５８】

利用許可証依頼処理部１８０４は、消費者あるいは他のリテーラから送信され

た利用許可証依頼を処理し、センタへの利用許可証依頼を作成し、入出力制御部１８０１経由でセンタへ送付する機能を持ち、処理制御部２２０１、署名検証部２２０２、エラーメッセージ作成部２２０３、利用許可証依頼作成部２２０４、署名作成部２２０５、利用条件作成部２２０６から構成される。

【０３５９】

利用許可証依頼処理部１８０４を構成する各部の役割を以下に述べる。

【０３６０】

処理制御部２２０１：処理選択部１８０２からの入力、入出力制御部１８０１への出力、仲介許諾証ＤＢ１８０７の参照、利用許可証仲介履歴ＤＢ１８０８へのエントリの追加の機能を担うとともに、利用許可証依頼の処理全体を制御する。

署名検証部２２０２：処理選択部１８０２から入力される利用許可証依頼のデジタル署名を検証する。

エラーメッセージ作成部２２０３：エラーメッセージを作成する。

利用許可証依頼作成部２２０４：センタへ送付する利用許可証依頼を作成する。利用許可証依頼にデジタル署名を添付するために署名作成部２２０５を呼び出す。さらに、リテーラの署名の検証鍵の公開鍵証明証を入手するために証明証記憶部１８１０にアクセスする。

署名作成部２２０５：利用許可証依頼作成部２２０４で作成する利用許可証依頼のためのデジタル署名を作成する。デジタル署名のための署名鍵を入手するために、署名鍵記憶部１８０９にアクセスする。

利用条件作成部２２０６：依頼する利用許可証に含まれるべき利用条件を作成する。

【０３６１】

図２３は、本実施例のリテーラが持つ利用許可証依頼処理部１８０４の処理制御部２２０１の動作を示すフローチャートである。処理制御部２２０１の動作を図２３にしたがって説明する。

【０３６２】

まず、処理選択部１８０２から入力された利用許可証依頼のデジタル署名を検証する（２３０１）。検証鍵は該利用許可証依頼の証明証フィールドに添付され

ているものを使用するが、必要な公開鍵証明証が証明証フィールドに存在しない場合には、ＣＡ１０８から公開鍵証明証を取得してから署名の検証を行う。

【０３６３】

署名の検証に失敗した場合、エラーメッセージ作成部２２０３でエラーメッセージを作成して入出力制御部１８０１に出力した後（２３０７）、終了する。

【０３６４】

署名の検証に成功した場合、入力された利用許可証依頼で利用許可証の仲介を依頼されている検証用公開鍵の仲介が許諾されているかどうかを検査する（２３０２）。仲介許諾証ＤＢ１８０７に、利用許可証依頼で依頼された検証用公開鍵に対する仲介許諾証が存在し、かつ、利用許可証依頼に記載されている利用条件が、仲介許諾証ＤＢ１８０７に保持されている仲介許諾証に記載されている利用条件限定情報の範囲内である場合に許諾されていると判断する。

【０３６５】

２３０２の検査で仲介が許諾されていないと判断された場合、エラーメッセージ作成部２２０３でエラーメッセージを作成して入出力制御部１８０１に出力した後（２３０７）、終了する。

【０３６６】

２３０２の検査で仲介が許諾されていると判断された場合、利用許可証依頼を受け付けるかどうかを判断する（２３０３）。入力された利用許可証依頼の発信者である消費者やリテーラが信用できない場合は、ここで利用許可証依頼を受け付けないことを決定する。

【０３６７】

２３０３で利用許可証依頼を受け付けないと判断した場合、エラーメッセージ作成部２２０３でエラーメッセージを作成して入出力制御部１８０１に出力した後（２３０７）、終了する。

【０３６８】

２３０３で利用許可証依頼を受け付けると判断した場合、利用条件作成部２２０６を呼び出し、センタへ送付する利用許可証依頼に記載する利用条件を作成させ、その結果を受けとる（２３０４）。利用条件作成部２２０６が作成する利用

条件は、入力された利用許可証依頼に記載されている利用条件のままでもよいし、必要ならリテーラの裁量で適切なものに修正してもよい。

【０３６９】

利用条件が決まったら、処理中の利用許可証依頼に関する情報を保持したエントリを利用許可証仲介履歴ＤＢ１８０８に追加する（２３０５）。新しいエントリの各属性には以下の値が設定される。

【０３７０】

【表３９】

利用許可証識別子属性：この時点では値は設定されない。

公開鍵識別子属性：入力された利用許可証依頼に含まれる許可仕様の公開鍵識別子フィールドに記載されている値。

プロバイダ識別子属性：公開鍵識別子属性に設定された識別子で特定される検証用公開鍵情報のユーザであるプロバイダの識別子。該プロバイダの識別子は、仲介許諾証ＤＢを参照して得ることができる。すなわち、本ＤＢの公開鍵識別子属性に設定された識別子を仲介許諾証ＤＢの公開鍵識別子属性の値に持つ仲介許諾証ＤＢのエントリのプロバイダ識別子属性がそれにあたる。

消費者識別子属性：入力された利用許可証依頼に含まれる許可仕様の消費者識別子フィールドの値。

依頼者識別子属性：入力された利用許可証依頼の発信者フィールドの値。

利用条件属性：２３０４で決定した利用条件。

依頼日時属性：入力された利用許可証依頼の日時フィールドの値。

発信日時属性：この時点では値は設定されない。

【０３７１】

最後にセンタへ送付する利用許可証依頼を作成し、入出力制御部１８０１を介してセンタに送付し（２３０６）、終了する。センタへ送付する利用許可証依頼の各フィールドには以下の値が設定される。

【０３７２】

【表４０】

発信者フィールド：自分自身すなわちリテーラの識別子。

受信者フィールド：センタの識別子。

日時フィールド：現在の日時。

許可内容フィールド：後述する許可仕様。

デジタル署名フィールド：このフィールドおよび証明証フィールド以外のフィールドのデータに対するデジタル署名。デジタル署名の作成のため、署名作成部２２０５を呼び出して署名値を作成させ、結果をこのフィールドに設定する。署名鍵は署名鍵記憶部１８０９にアクセスして入手する。

証明証フィールド：証明証記憶部１８１０に記憶している公開鍵証明証。

【０３７３】

許可内容フィールドに記載される許可仕様の各フィールドには、以下の値が記載される。

【０３７４】

【表４１】

公開鍵識別子フィールド：入力された利用許可証依頼に含まれる許可仕様に記載された公開鍵識別子フィールドの値。

消費者識別子フィールド：入力された利用許可証依頼に含まれる許可仕様に記載された消費者識別子フィールドの値。

利用条件フィールド：２３０４で決定した利用条件。

仲介許諾フィールド：仲介許諾証ＤＢ１８０７に保持されている、利用許可証依頼で依頼された検証用公開鍵に対する仲介許諾証。

【０３７５】

［利用許可証送付処理部］

図２４は、本実施例のリテーラが持つ利用許可証送付処理部１８０６の内部構成を示した図である。

【０３７６】

利用許可証送付処理部１８０６は、センタあるいは他のリテーラからの送信された利用許可証送付を処理し、利用許可証の依頼者に送付する利用許可証送付を作成し、入出力制御部１８０１経由で該依頼者に送付する機能を持ち、処理制御部２４０１、署名検証部２４０２、エラーメッセージ作成部２４０３、利用許可

証送付作成部２４０４、署名作成部２４０５から構成される。

【０３７７】

利用許可証送付処理部１８０６を構成する各部の役割を以下に述べる。

【０３７８】

処理制御部２４０１：処理選択部１８０２からの入力、入出力制御部１８０１への出力、利用許可証仲介履歴ＤＢ１８０８のエントリ更新の機能を担うとともに、利用許可証送付の処理全体を制御する。

署名検証部２４０２：処理選択部１８０２から入力される利用許可証送付、および利用許可証送付に含まれる利用許可証のデジタル署名を検証する。

エラーメッセージ作成部２４０３：エラーメッセージを作成する。

利用許可証送付作成部２４０４：利用許可証の依頼者に送付する利用許可証送付を作成する。新たに作成する利用許可証送付にデジタル署名を添付するために署名作成部２４０５を呼び出す。さらに、リテーラの署名の検証鍵の公開鍵証明証を入手するために証明証記憶部１８１０にアクセスする。

署名作成部２４０５：利用許可証送付作成部２４０４で作成する利用許可証送付のためのデジタル署名を作成する。デジタル署名のための署名鍵を入手するために、署名鍵記憶部１８０９にアクセスする。

【０３７９】

図２５は、本実施例のリテーラが持つ利用許可証送付処理部１８０６の処理制御部２４０１の動作を示すフローチャートである。処理制御部２４０１の動作を図２５にしたがって説明する。

【０３８０】

まず、処理選択部１８０２から入力された利用許可証送付および該利用許可証送付に含まれる利用許可証のデジタル署名を検証する（２５０１）。検証鍵は該利用許可証送付の証明証フィールドに添付されているものを使用するが、必要な公開鍵証明証が証明証フィールドに存在しない場合には、ＣＡ１０８から公開鍵証明証を取得してから署名の検証を行う。

【０３８１】

署名の検証に失敗した場合、エラーメッセージ作成部２４０３でエラーメッセ

ージを作成して入出力制御部１８０１に出力した後（２５０４）、終了する。

【０３８２】

署名の検証に成功した場合、入力された利用許可証送付で送付された内容にしたがって、利用許可証仲介履歴ＤＢ１８０８のエントリを更新する（２５０２）。更新されるエントリは、入力された利用許可証送付に対応する利用許可証依頼を処理した時に追加されたエントリであり、エントリの公開鍵識別子属性、消費者識別子属性の値が、それぞれ入力された利用許可証送付に含まれる利用許可証の公開鍵識別子フィールド、受領者フィールドの値と一致し、該エントリの利用許可証識別子属性と発信日時属性の値が設定されていないものである。

【０３８３】

更新対象のエントリの各属性は以下のように更新される。

【０３８４】

【表４２】

利用許可証識別子属性：入力された利用許可証送付に含まれる利用許可証の利用許可証識別子フィールドの値。

公開鍵識別子属性：変化なし。

プロバイダ識別子属性：変化なし。

消費者識別子属性：変化なし。

依頼者識別子属性：変化なし。

利用条件属性：入力された利用許可証送付に含まれる利用許可証の利用条件フィールドの値。

依頼日時属性：変化なし。

発信日時属性：現在の時刻。

【０３８５】

最後に、利用許可証の依頼者に送付する新たな利用許可証送付を作成し、入出力制御部１８０１を介して利用許可証の依頼者に送付し（２５０３）、終了する。新たに作成される利用許可証送付の各フィールドには以下の値が設定される。

【０３８６】

【表４３】

発信者フィールド：自分自身すなわちリテーラの識別子。

受信者フィールド：２５０２で更新された利用許可証仲介履歴ＤＢ１８０８のエントリの依頼者識別子属性の値。

日時フィールド：２５０２で更新された利用許可証仲介履歴ＤＢ１８０８のエントリの発信日時属性の値。

利用許可証フィールド：入力された利用許可証送付に含まれる利用許可証。

デジタル署名フィールド：このフィールドおよび証明証フィールド以外のフィールドのデータに対するデジタル署名。デジタル署名の作成のため、署名作成部２４０５を呼び出し、結果の署名値を受け取り、このフィールドに設定する。

証明証フィールド：証明証記憶部１８１０に記憶している公開鍵証明証と、入力された利用許可証送付の証明証フィールドに含まれる証明証のうち、該利用許可証送付に含まれる利用許可証のデジタル署名を検証できる検証鍵を含む公開鍵証明証。

【０３８７】

［利用許可証依頼処理の課金・決済］

本実施例のリテーラは、利用許可証依頼の処理の過程で利用許可証発行料金の課金あるいは決済を行うことができる。課金あるいは決済の処理は、消費者からの利用許可証依頼をうけた後、センタに利用許可証依頼を送付する前に行われる。

【０３８８】

課金の場合は、利用許可証依頼の処理の過程で、消費者毎に利用許可証発行料金を加算しておき、後に消費者に対して請求する。そのため、本実施例のリテーラは、消費者毎に現在の利用許可証発行料金高を保持するデータベースをもっている。

【０３８９】

本実施例のリテーラは、利用許可証依頼の処理のたび毎に利用許可証発行料金の決済を行うこともできる。決済の方法としては、消費者が所持するクレジットカードによる決済や、プリペイドの方式等種々のものが利用可能であるが、いずれも、消費者からの利用許可証依頼をうけた後、決済が終了した事が確認されて

から、センタに利用許可証依頼を送付する。

【０３９０】

［リテーラが発行する履歴情報］

本実施例のリテーラは利用許可証仲介の履歴情報をプロバイダに送付する事ができる。

【０３９１】

プロバイダに渡される利用許可証仲介の履歴情報は、そのプロバイダに割り当てられた検証用公開鍵に対応する利用許可証の仲介についての情報であり、利用許可証仲介プロバイダ用履歴作成部１８１１で作成され、入出力制御部１８０１を介してプロバイダに送付される。この履歴は、リテーラがプロバイダに送付するマージンの額に対する根拠となる。

【０３９２】

利用許可証仲介プロバイダ用履歴作成部１８１１は、履歴を作成するプロバイダの識別子と履歴作成の対象期間の開始日時と終了日時の指定を受け、利用許可証仲介履歴ＤＢ１８０８から、プロバイダ識別子属性の値が指定されたプロバイダの識別子と一致し、発行日属性の値が指定された履歴作成の対象期間内であるエントリ群を取り出し、その利用許可証識別子属性、公開鍵識別子属性、利用条件属性、依頼日時属性、発信日時属性の値を取り出す。本実施例では、履歴を作成するプロバイダの識別子と履歴作成の対象期間の指定はリテーラのオペレータから受けるが、インターネット経由でプロバイダから入力されるように構成してもよい。

【０３９３】

また、本実施例のリテーラは利用許可証仲介の履歴情報を利用許可証仲介の依頼者にも送付する事ができる。

【０３９４】

依頼者に渡される利用許可証仲介の履歴情報は、その依頼者から依頼された利用許可証の仲介についての情報であり、利用許可証仲介依頼者用履歴作成部１８１２で作成され、入出力制御部１８０１を介して依頼者に送付される。この履歴は、リテーラが依頼者に対して手数料の請求を行う場合の根拠となる。

【０３９５】

利用許可証仲介依頼者用履歴作成部１８１２は、履歴を作成する依頼者の識別子と履歴作成の対象期間の開始日時と終了日時の指定を受け、利用許可証仲介履歴ＤＢ１８０８から、依頼者識別子属性の値が指定されたプロバイダの識別子と一致し、発行日属性の値が指定された履歴作成の対象期間内であるエントリ群を取り出し、その利用許可証識別子属性、公開鍵識別子属性、プロバイダ識別子属性、消費者識別子属性、利用条件属性、依頼日時属性、発信日時属性の値を取り出す。本実施例では、履歴を作成する依頼者の識別子と履歴作成の対象期間の指定はリテーラのオペレータから受けるが、インターネット経由で依頼者から入力されるように構成してもよい。

【０３９６】

上記の履歴情報のプロバイダや依頼者への送付方法は、電子メールでもよいし、ＷＷＷベースでオンデマンドで発行してもよい。盗聴や改竄の危険がある場合は暗号化やデジタル署名が適用されるのが望ましい。

【０３９７】

［消費者端末の構成］

図２６は、本実施例の消費者端末の構成図である。

【０３９８】

本実施例の消費者は、消費者識別子と消費者秘密情報を内蔵した携帯型記憶装置を所持しており、インターネットを介してリテーラから利用許可証を受け取って該携帯型記憶装置に記憶する。消費者端末は、入出力制御部２６０２、利用許可証依頼作成部２６０３、利用許可証送付処理部２６０４、署名鍵記憶部２６０５、証明証記憶部２６０６、携帯型記憶装置制御部２６０７から構成され、入出力制御部２６０２を介してインターネットに接続されているとともに、携帯型記憶装置制御部２６０７を介して携帯型記憶装置と接続されている。

【０３９９】

本実施例の消費者端末の各部の役割を以下に述べる。

【０４００】

入出力制御部２６０２：インターネットを介したデータの入力を受け付けるとと

もに、利用許可証依頼作成部２６０３が作成した利用許可証依頼をインターネットを介して出力する。インターネットからの入出力制御部２６０２への入力、あるいは、入出力制御部２６０２からインターネットへの出力の方法としては、他のエンティティが用意しているWWWサイトにアクセスして消費者端末が作成したデータを送るもの、あるいは電子メールシステムと入出力制御部２６０２を自動的にあるいは人手によって連動させるものなどが使用できる。

【０４０１】

利用許可証依頼作成部２６０３：利用許可証依頼を作成し、入出力制御部２６０２を介してリテーラに送付する。利用許可証依頼の作成の過程で、署名鍵記憶部２６０５と証明証記憶部２６０６にアクセスするとともに、携帯型記憶装置制御部２６０７を介して携帯型記憶装置２６０８にアクセスする。

利用許可証送付処理部２６０４：リテーラからの利用許可証送付を処理し、該利用許可証送付に含まれている利用許可証を携帯型記憶装置制御部２６０７を介して携帯型記憶装置２６０８に記録する。

署名鍵記憶部２６０５：消費者端末が作成するデジタル署名に使用する署名鍵を保持する。

証明証記憶部２６０６：署名鍵記憶部２６０５に記憶されている署名鍵で作成したデジタル署名を検証できる検証鍵を含む公開鍵証明証を保持する。

携帯型記憶装置制御部２６０７：携帯型記憶装置２６０８へのデータの書込みとアクセスを行う。

【０４０２】

本実施例では、利用許可証依頼にデジタル署名を施す場合に使用する署名鍵や、その署名鍵で作成した署名を検証する検証鍵を含む公開鍵証明証は、消費者端末が保持しているものとしたが、これらが携帯型記憶装置に保持されているように構成してもよい。

【０４０３】

本実施例では、消費者が携帯型記憶装置を所持しており、該記憶装置に利用許可証を記憶するように構成しているが、もちろん、消費者端末自体の記憶領域に記憶するように構成してもよい。

【０４０４】

［利用許可証依頼作成部］

本実施例の消費者端末は、該端末を利用している消費者が利用したいデジタルコンテンツがある場合、そのデジタルコンテンツの利用許可証の仲介を依頼する利用許可証依頼を利用許可証依頼作成部２６０３で作成し、入出力制御部２６０２を介してリテーラに送付する。

【０４０５】

利用許可証依頼作成部２６０３では、利用許可証依頼の各フィールドに以下の値を設定する。

【０４０６】

【表４４】

発信者フィールド：自分自身すなわち消費者端末の識別子。

受信者フィールド：リテーラの識別子。

日時フィールド：現在の時刻。

許可内容フィールド：後述する許可仕様。

デジタル署名フィールド：このフィールドおよび証明証フィールド以外のフィールドのデータに対するデジタル署名。デジタル署名の作成のため、利用許可証依頼作成部２６０３は署名作成部を含んでおり、この署名作成部が作成した署名値をこのフィールドに設定する。署名鍵は署名鍵記憶部２６０５にアクセスして入手する。

証明証フィールド：証明証記憶部２６０６に記憶している公開鍵証明証。

【０４０７】

許可内容フィールドに指定される許可仕様の各フィールドには以下の値が設定される。

【０４０８】

【表４５】

公開鍵識別子フィールド：利用したいデジタルコンテンツに割り当てられている検証用公開鍵の識別子。

消費者識別子フィールド：消費者端末を使用している消費者の識別子。消費者識

別子は携帯型記憶装置２６０８に記憶されており、利用許可証依頼作成部２６０３は、携帯型記憶装置制御部２６０７を介して携帯型記憶装置２６０８から消費者識別子を入手する。

利用条件フィールド：消費者の希望等を反映した適切なものを利用許可証依頼作成部２６０３が決定して設定。

仲介許諾証フィールド：設定しない。

【０４０９】

［利用許可証送付処理部］

利用許可証依頼作成部２６０３で利用許可証依頼が作成されリテーラに送付されると、その返信としてリテーラから利用許可証送付が送信されてくる。利用許可証送付は、入出力制御部２６０２を経由して利用許可証送付処理部２６０４に入力され、そこで処理される。

【０４１０】

図２７は、本実施例の消費者端末が持つ利用許可証依頼作成部２６０３の動作を示すフローチャートである。利用許可証依頼作成部２６０３の動作を図２７にしたがって説明する。

【０４１１】

まず、入力された利用許可証送付および該利用許可証送付に含まれる利用許可証のデジタル署名を検証する（２７０１）。検証鍵は検証用公開鍵情報送付の証明証フィールドに添付されているものを使用するが、必要な公開鍵証明証が証明証フィールドに存在しない場合には、ＣＡ１０８から公開鍵証明証を取得してから署名の検証を行う。

【０４１２】

２７０１で、デジタル署名の検証に失敗した場合、エラー処理を行った後（２７０４）、終了する。

【０４１３】

２７０１で、デジタル署名の検証に成功した場合、入力された利用許可証送付に含まれる利用許可証が、現在消費者端末を使用している消費者向けのものかどうかが検査される（２７０２）。検査は、携帯型記憶装置制御部２６０７を介し

て携帯型記憶装置２６０８から入手した消費者識別子と、入力された利用許可証送付に含まれる利用許可証の受領者フィールドの値が一致するかどうかで行われる。

【０４１４】

２７０２の検査で、入力された利用許可証送付に含まれる利用許可証が現在消費者端末を使用している消費者向けのものでないと判断された場合、エラー処理を行った後（２７０４）、終了する。

【０４１５】

２７０２の検査で、入力された利用許可証送付に含まれる利用許可証が現在消費者端末を使用している消費者向けのものであると判断された場合、該利用許可証を携帯型記憶装置制御部２６０７を介して携帯型記憶装置２６０８に記録し（２７０３）、終了する。

本実施例では、消費者が携帯型記憶装置を所持し、そこに消費者識別子が記憶されているが、これが消費者端末中の記憶領域に記憶されるよう構成してもよい。

【０４１６】

【発明の効果】

以上説明したように、この発明によれば、デジタルコンテンツ提供者が利用証明証を発行するファシリティの構築や維持管理からデジタルコンテンツ提供者が開放される。

【図面の簡単な説明】

【図１】本発明を適用した実施例の構成図である。

【図２】本発明を適用したセンタの構成図である。

【図３】本発明を適用したセンタの動作を示すフローチャートである。

【図４】本発明を適用したセンタが持つ検証用公開鍵情報依頼処理部の内部構成を示した図である。

【図５】本発明を適用したセンタが持つ検証用公開鍵情報依頼処理部の処理制御部の動作を示すフローチャートである。

【図６】本発明を適用したセンタが持つプロバイダＤＢの構造を示した図で

ある。

【図７】本発明を適用したセンタが持つ公開鍵ペアＤＢの構造を示した図である。

【図８】本発明を適用したセンタが持つリテーラＤＢの構造を示した図である。

【図９】本発明を適用したセンタが持つ消費者ＤＢの構造を示した図である。

【図１０】本発明を適用したセンタが持つ利用許可証発行履歴ＤＢの構造を示した図である。

【図１１】本発明を適用したセンタが持つ利用許可証依頼処理部の内部構成を示した図である。

【図１２】本発明を適用したセンタが持つ利用許可証依頼処理部の処理制御部の動作を示すフローチャートである。

【図１３】本発明を適用したプロバイダの構成図である。

【図１４】本発明を適用したプロバイダが持つ検証用公開鍵ＤＢの構造を示した図である。

【図１５】本発明を適用したプロバイダが持つ検証用公開鍵情報送付処理部の動作を示すフローチャートである。

【図１６】本発明を適用したプロバイダが持つ仲介許諾証依頼処理部の内部構成を示した図である。

【図１７】本発明を適用したプロバイダが持つ仲介許諾証依頼処理部の処理制御部の動作を示すフローチャートである。

【図１８】本発明を適用したリテーラの構成図である。

【図１９】本発明を適用したリテーラが持つ仲介許諾証ＤＢの構造を示した図である。

【図２０】本発明を適用したリテーラが持つ利用許可証仲介履歴ＤＢの構造を示した図である。

【図２１】本発明を適用したリテーラが持つ仲介許諾証送付処理部の動作を示すフローチャートである。

【図２２】本発明を適用したリテーラが持つ利用許可証依頼処理部の内部構成を示した図である。

【図２３】本発明を適用したリテーラが持つ利用許可証依頼処理部の処理制御部の動作を示すフローチャートである。

【図２４】本発明を適用したリテーラが持つ利用許可証送付処理部の内部構成を示した図である。

【図２５】本発明を適用したリテーラが持つ利用許可証送付処理部の処理制御部の動作を示すフローチャートである。

【図２６】本発明を適用した消費者端末の構成図である。

【図２７】本発明を適用した消費者端末が持つ利用許可証依頼作成部の動作を示すフローチャートである。

【図２８】本発明を適用した携帯型記憶装置と利用許可証検査機能付きソフトウエアの内部構成例を示した図である。

【図２９】利用許可証の検証の際の携帯型記憶装置と利用許可証検証機能付きソフトウエア動作を示すフローチャートである。

【図３０】本発明を適用した利用許可証検査機能付きコンテンツプロセッシングソフトウエアと利用許可証明部の内部構成例を示した図である。

【図３１】利用許可証の検証の際の利用許可証検査機能付きコンテンツプロセッシングソフトウエアと利用許可証明部の動作を示すフローチャートである。

【図３２】本発明を適用した利用許可証検査機能付きコンテンツ復号ソフトウエアと利用許可証明部の内部構成例を示した図である。

【図３３】利用許可証の検証の際の利用許可証検査機能付きコンテンツ復号ソフトウエアと利用許可証明部の動作を示すフローチャートである。

【図３４】本発明を適用したプロバイダが持つ仲介許諾証発行履歴ＤＢの構造を示した図である。

【図３５】本発明を適用した利用許可証検査機能付きソフトウエアの構成例を示した図である。

【図３６】本発明を適用した利用許可証検査機能付きコンテンツプロセッシングソフトウエアの構成例を示した図である。

【図３７】本発明を適用した利用許可証検査機能付きコンテンツプロセッシングソフトウエアで操作されるデジタルコンテンツのデータ構造を示した図である。

【図３８】本発明を適用した利用許可証検査機能付きコンテンツ復号ソフトウエアの構成例を示した図である。

【図３９】発明を適用した利用許可証検査機能付きコンテンツ復号ソフトウエアで復号されるデジタルコンテンツのデータ構造を示した図である。

【符号の説明】

１０１　インターネット１０１
１０３、１０４　リテーラ
１０２　利用許可証発行センタ
１０５、１０６　プロバイダ
１０７　消費者端末
１０８　認証局（Ｃｅｒｔｉｆｉｃａｔｅ　Ａｕｔｈｏｒｉｔｙ）
２０１　入出力制御部
２０２　処理選択部
２０３　検証用公開鍵情報依頼処理部
２０４　利用許可証依頼処理部
２０５　プロバイダＤＢ
２０６　公開鍵ペアＤＢ
２０７　リテーラＤＢ
２０８　消費者ＤＢ
２０９　利用許可証発行履歴ＤＢ
２１０　署名鍵記憶部
２１１　証明証記憶部
２１２　利用許可証発行プロバイダ用履歴作成部
２１３　利用許可証発行リテーラ用履歴作成部
２１４　検証用公開鍵情報発行履歴作成部
４０１　処理制御部

４０２　署名検証部

４０３　公開鍵ペア作成部

４０４　公開鍵ペア識別子作成部

４０５　検証用公開鍵情報作成部

４０６　検証用公開鍵情報送付作成部

４０７　エラーメッセージ作成部

４０８　署名作成部

１１０１　処理制御部

１１０２　署名検証部

１１０３　仲介許諾内容確認部

１１０４　利用許可証識別子作成部

１１０５　利用許可証作成部

１１０６　利用許可証送付作成部

１１０７　エラーメッセージ作成部

１１０８　署名作成部

１１０９　証明値作成部

１１１０　利用条件作成部

１３０１　入出力制御部

１３０２　処理選択部

１３０３　検証用公開鍵情報依頼作成部

１３０４　検証用公開鍵情報送付処理部

１３０５　仲介許諾証依頼処理部

１３０６　検証用公開鍵ＤＢ

１３０７　署名鍵記憶部

１３０８　証明証記憶部

１３０９　仲介許諾証発行履歴ＤＢ

１３１０　仲介許諾証発行履歴作成部

１８０１　入出力制御部

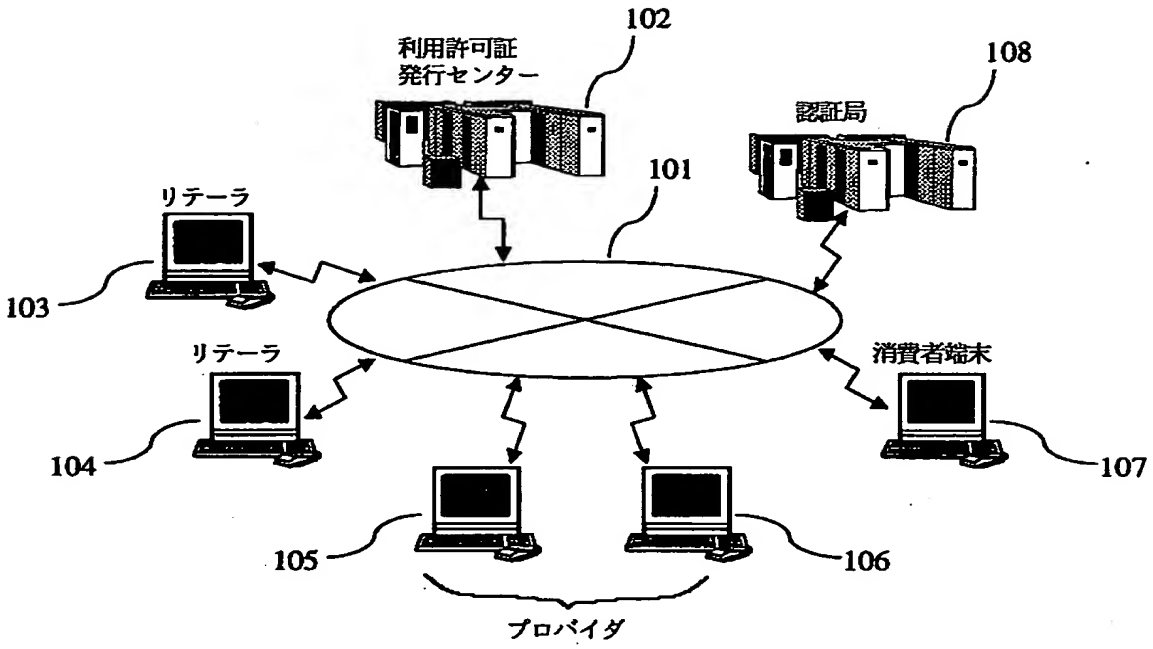
１８０２　処理選択部

１８０３　仲介許諾証依頼作成部
１８０４　利用許可証依頼処理部
１８０５　仲介許諾証送付処理部
１８０６　利用許可証送付処理部
１８０７　仲介許諾証ＤＢ
１８０８　利用許可証仲介履歴ＤＢ
１８０９　署名鍵記憶部
１８１０　証明証記憶部
１８１１　利用許可証仲介プロバイダ用履歴作成部
１８１２　利用許可証仲介依頼者用履歴作成部
２６０２　入出力制御部
２６０３　利用許可証依頼作成部
２６０４　利用許可証送付処理部
２６０５　署名鍵記憶部
２６０６　証明証記憶部
２６０７　携帯型記憶装置制御部
２８０１　条件判定対象情報生成部
２８０２　チャレンジ生成部
２８０３　公開鍵情報記憶部
２８０４　レスポンス検査部
２８１１　入出力制御部
２８１２　消費者秘密情報記憶部
２８１３　レスポンス計算部
２８１４　利用条件判定部
２８１５　利用許可証記憶部
３００１　入出力インタフェース
３００２　チャレンジ生成部
３００３　条件判定対象情報生成部
３００４　公開鍵情報記憶部

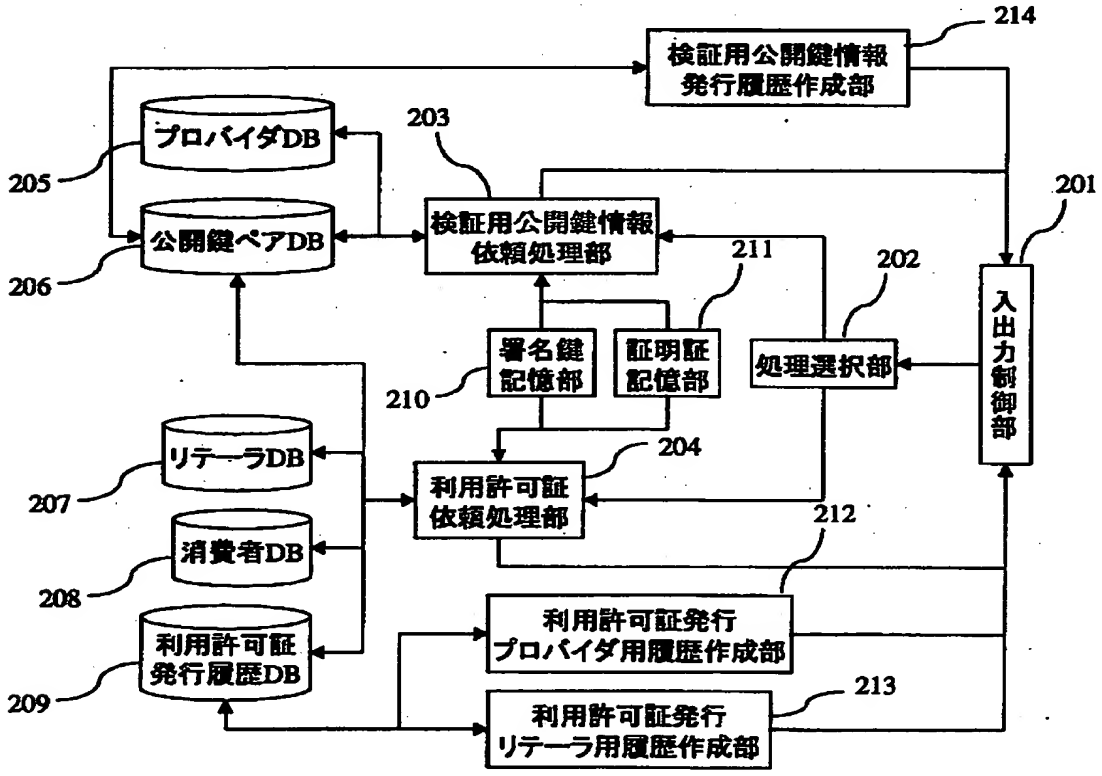
３００５　レスポンス検査部
３００６　利用条件判定部
３００７　利用許可証記憶部
３００８　通信制御部
３０１１　入出力制御部
３０１２　消費者秘密情報記憶部
３０１３　レスポンス計算部
３０１４　利用許可証記憶部
３５０１　利用対象のソフトウエア
３５０２　入出力制御部
３５０３　処理制御部
３５０４　第１の機能の実行部
３５０５　第２の機能の実行部
３５０６　第１の利用許可証検査部
３５０７　第２の利用許可証検査部
３５０８　携帯型記憶装置制御部
３５１１　携帯型記憶装置
３６０１　デジタルコンテンツプロセッシングソフトウエア
３６０２　入出力制御部
３６０３　処理制御部
３６０４　表示実行部
３６０５　編集実行部
３６０６　印刷実行部
３６０７　コンテンツデータ記憶部
３６０８　利用許可証検査部
３６１１　利用許可証明部

【書類名】　　図面

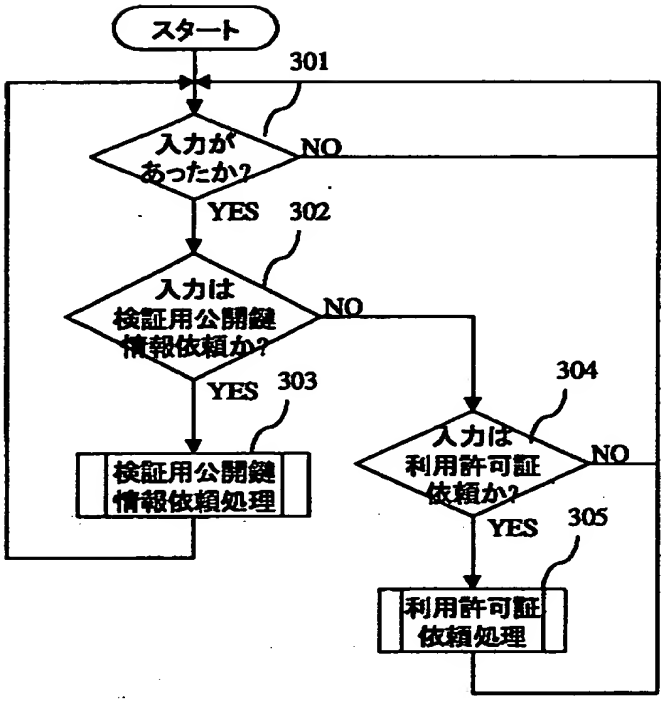
【図１】


102
利用許可証
発行センター
108
認証局
101
リテーラ
103
リテーラ
104
消費者端末
107
105
106
プロバイダ

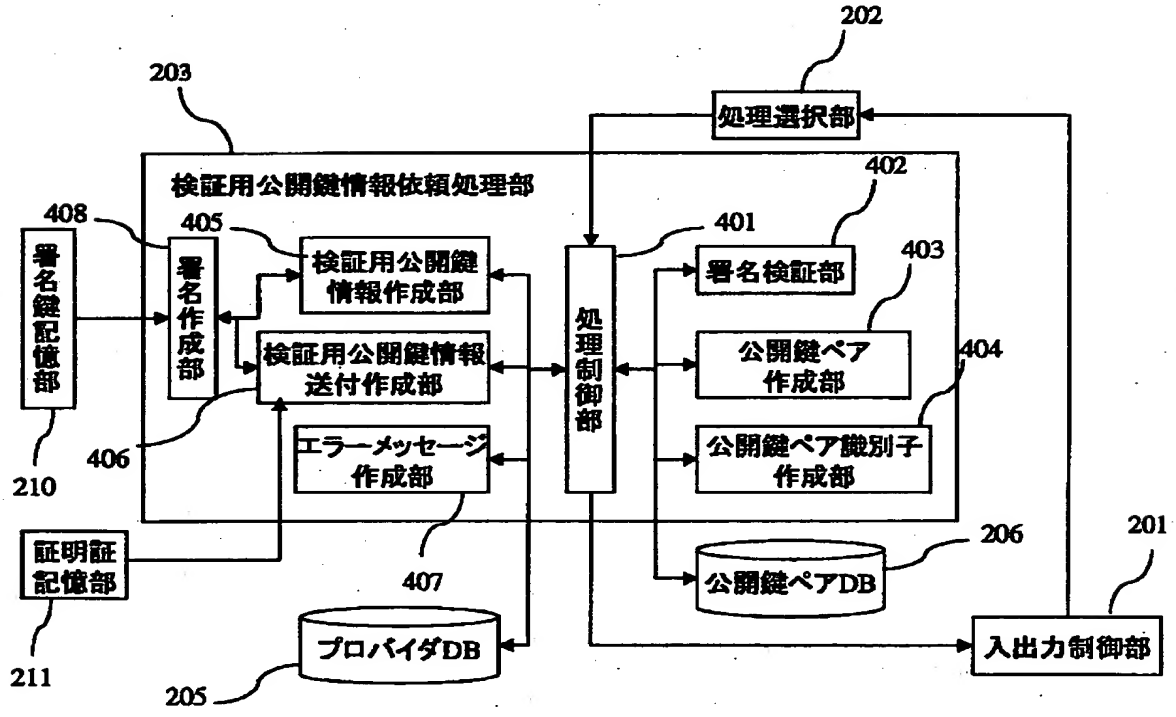
【図２】


214
検証用公開鍵情報
発行履歴作成部
プロバイダDB
205
203
201
公開鍵ペアDB
206
検証用公開鍵情報
依頼処理部
211
202
署名鍵
記憶部
210
証明証
記憶部
処理選択部
入出力制御部
リテーラDB
207
204
利用許可証
依頼処理部
212
消費者DB
208
利用許可証発行
プロバイダ用履歴作成部
利用許可証
発行履歴DB
209
213
利用許可証発行
リテーラ用履歴作成部

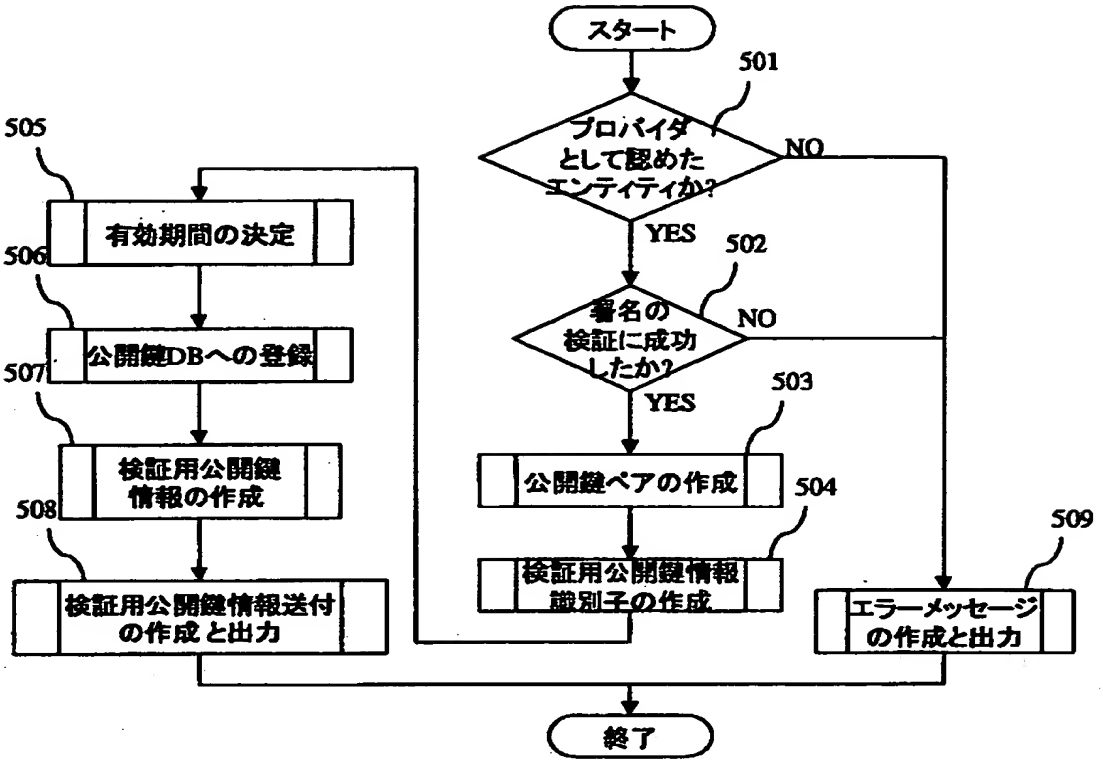
【図３】


スタート
301
入力があったか?
NO
YES
302
入力は検証用公開鍵情報依頼か?
NO
YES
303
検証用公開鍵情報依頼処理
304
入力は利用許可証依頼か?
NO
YES
305
利用許可証依頼処理

【図４】


202
処理選択部
203
検証用公開鍵情報依頼処理部
402
401
403
404
408
405
署名鍵記憶部
署名作成部
検証用公開鍵情報作成部
検証用公開鍵情報送付作成部
処理制御部
署名検証部
公開鍵ペア作成部
公開鍵ペア識別子作成部
210
406
エラーメッセージ作成部
407
206
201
証明証記憶部
公開鍵ペアDB
211
プロバイダDB
入出力制御部
205

【図５】



【図６】

プロバイダ識別子
PRV10001
PRV10002
PRV10003
...

【図７】

公開鍵識別子	法数	公開鍵	秘密鍵	プロバイダ識別子	有効期間開始	有効期間終了	発行日
PK00001	10110...	11001...	10101...	PRV10001	2000.1.1	2001.1.1	2000.12.1
PK00002	10010...	11110...	11011...	PRV10003	1999.3.5	2000.2.3	2000.1.2
PK00003	11111...	10000...	10101...	PRV10001	1999.11.1	2000.5.1	2000.3.1
...	...	...	...	...	...	...	...

【図８】

リテーラ識別子
RTL10001
RTL10002
RTL10003
...

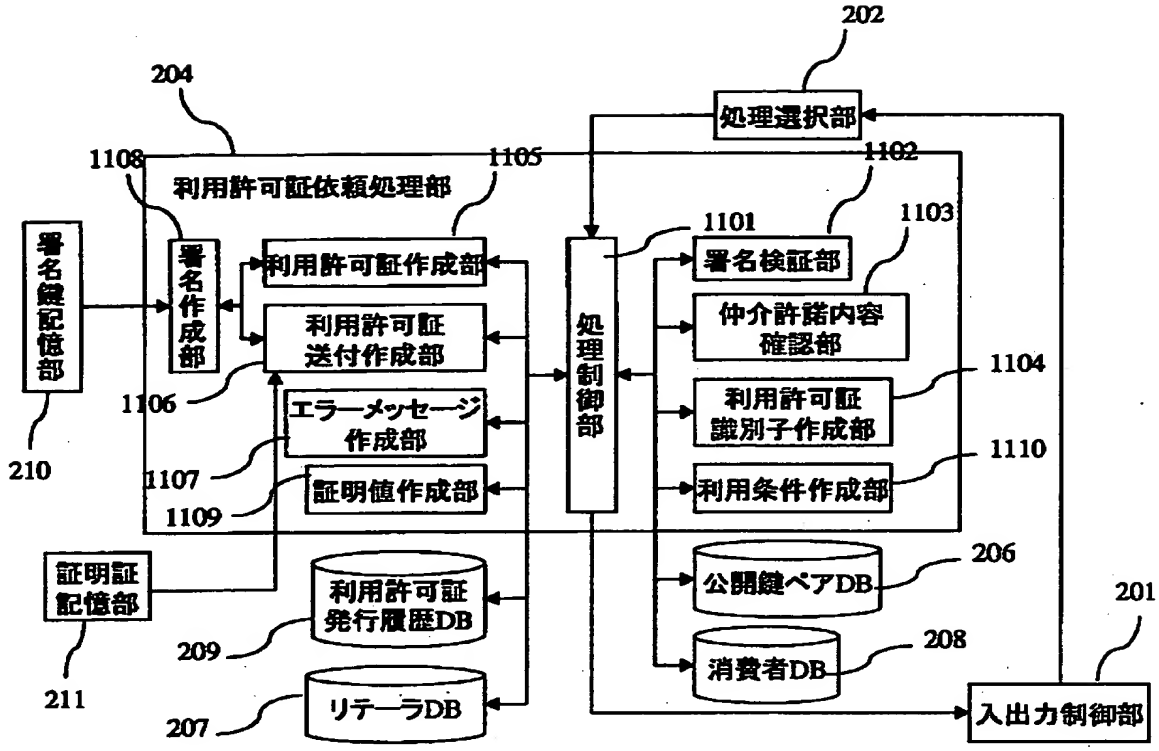
【図９】

消費者識別子	消費者秘密情報
CNS10001	10110...
CNS10002	11000...
CNS10003	01110...
...	...

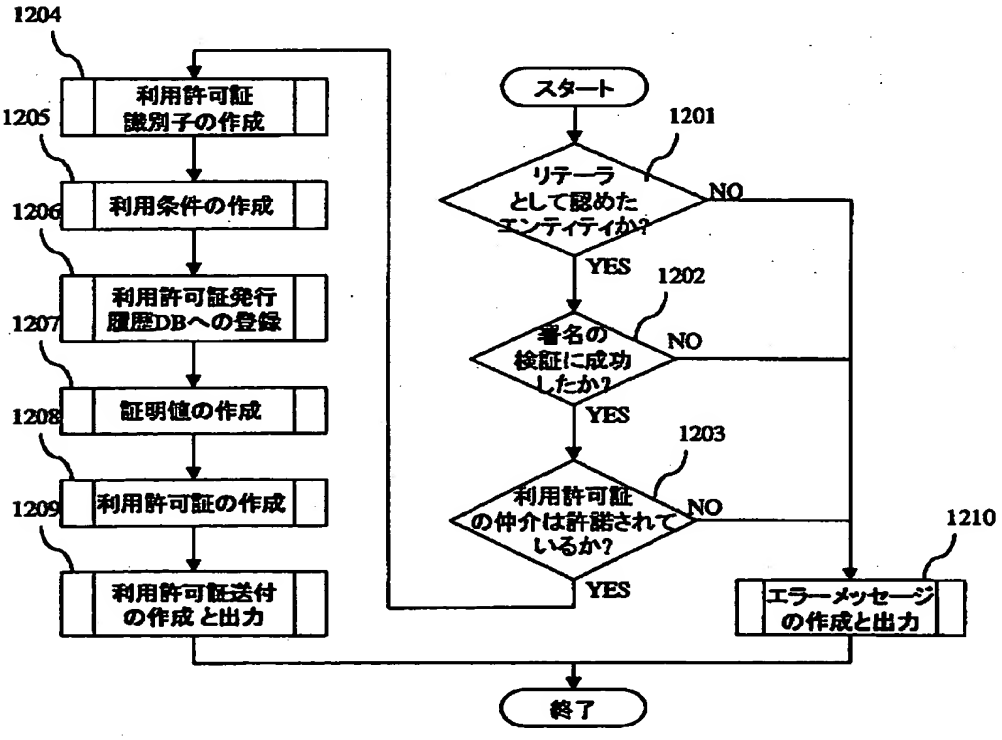
【図１０】

公開鍵識別子	プロバイダ識別子	消費者識別子	仲介者識別子	利用条件	発行日
PK00001	PRV10001	CNS10001	RTL10002	2F34A...	2000.2.1
PK00002	PRV10003	CNS10001	RTL10002	44FBC...	1999.4.16
PK00002	PRV10003	CNS10003	RTL10001	5AAB1...	1999.11.12
...	...	...	...	...	...

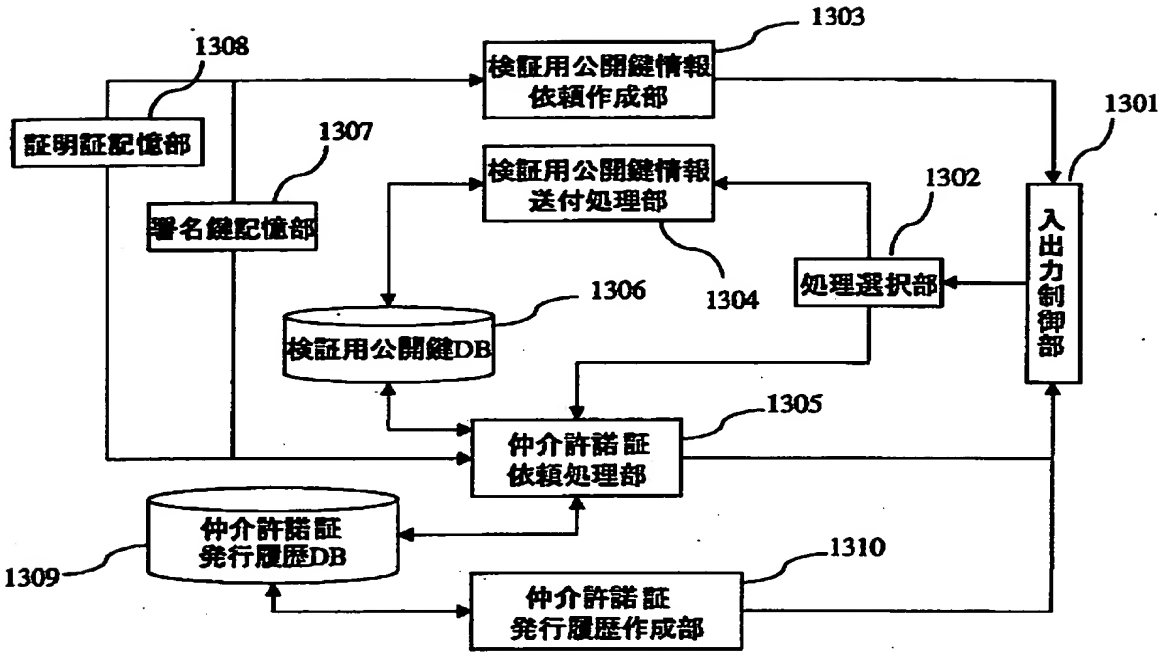
【図１１】


202
処理選択部
204
1108
利用許可証依頼処理部
1105
1102
1101
1103
署名鍵記憶部
署名作成部
利用許可証作成部
利用許可証送付作成部
処理制御部
署名検証部
仲介許諾内容確認部
1106
エラーメッセージ作成部
1104
利用許可証識別子作成部
210
1107
証明値作成部
1110
利用条件作成部
1109
証明証記憶部
利用許可証発行履歴DB
公開鍵ペアDB
206
201
209
消費者DB
208
211
リテーラDB
207
入出力制御部

【図１２】


1204
利用許可証識別子の作成
1205
利用条件の作成
1206
利用許可証発行履歴DBへの登録
1207
証明値の作成
1208
利用許可証の作成
1209
利用許可証送付の作成と出力
スタート
1201
リテーラとして認めたエンティティか?
NO
YES
1202
署名の検証に成功したか?
NO
YES
1203
利用許可証の仲介は許諾されているか?
NO
YES
1210
エラーメッセージの作成と出力
終了

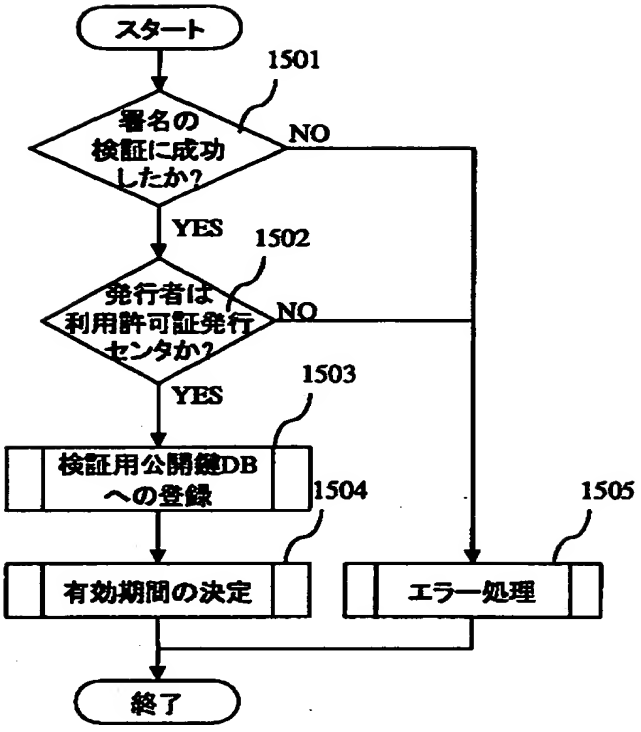
【図１３】



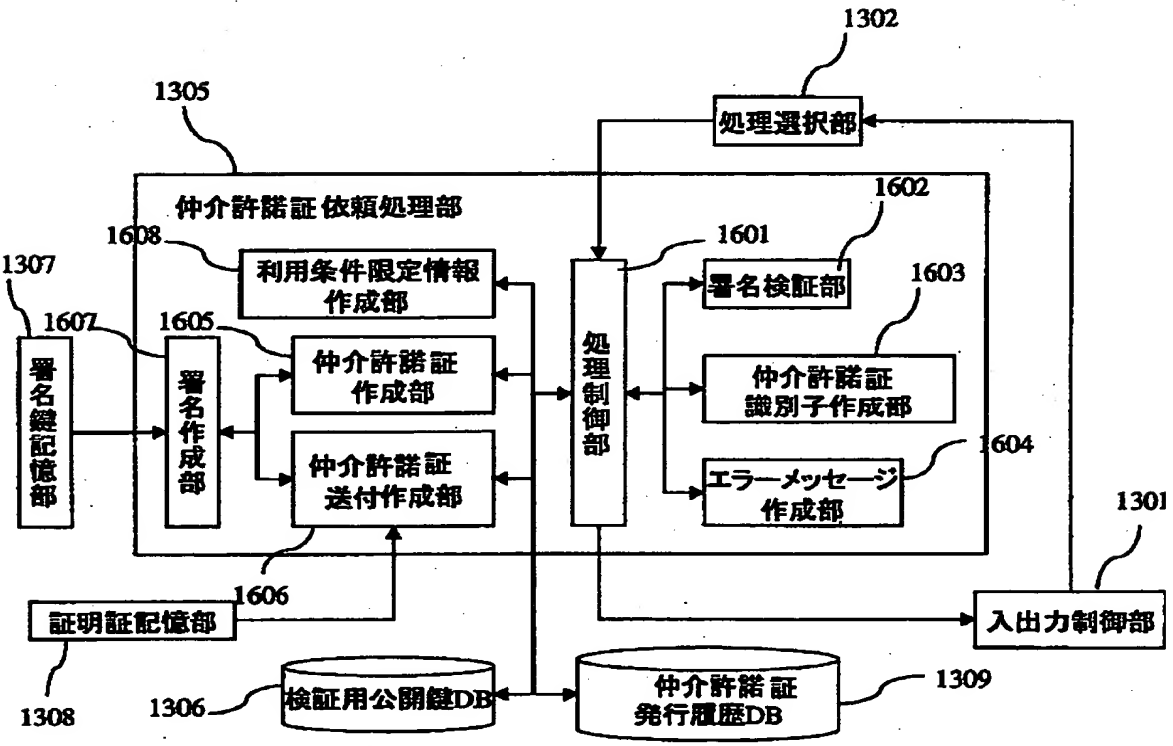
【図１４】

公開鍵識別子	法数	公開鍵	有効期間開始	有効期間終了	用途
PK00001	10110...	11001...	2000.1.1	2001.1.1	WD+++利用
PK00003	11111...	10000...	1999.11.1	2000.5.1	Mimic 写真集閲覧
PK00007	11000...	10110...	1999.8.1	2000.2.1	WJE 利用
...	...	...	...	...	...

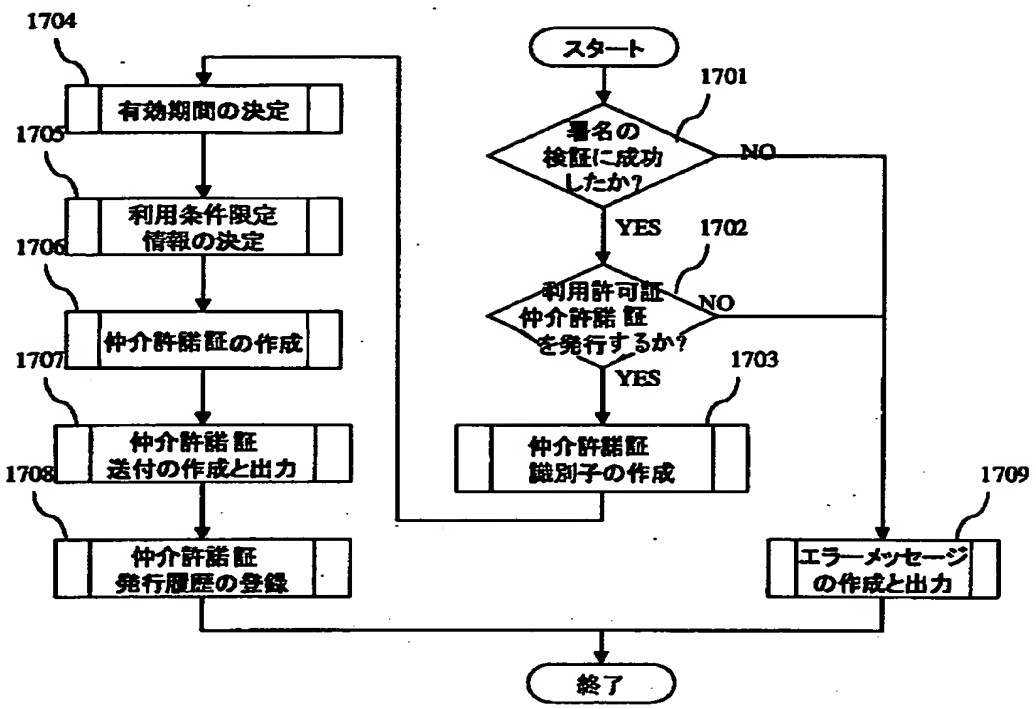
【図１５】


スタート
1501
署名の検証に成功したか?
NO
YES
1502
発行者は利用許可証発行センタか?
NO
YES
1503
検証用公開鍵DBへの登録
1504
1505
有効期間の決定
エラー処理
終了

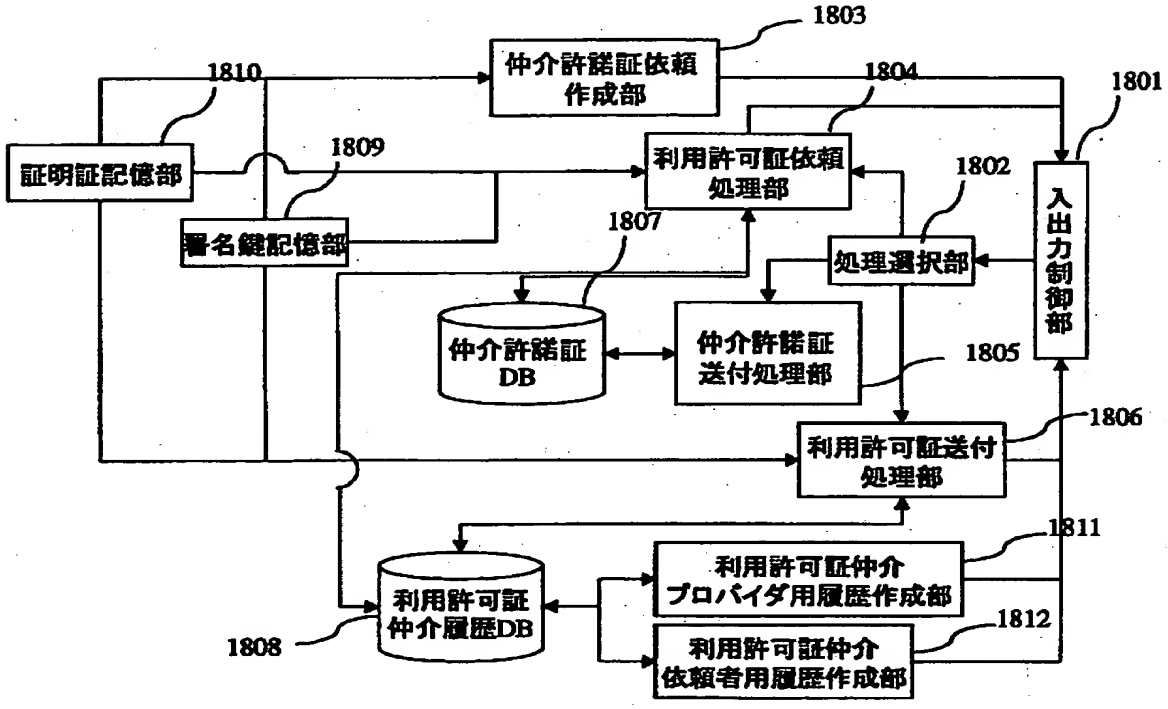
【図１６】


1302
処理選択部
1305
仲介許諾証依頼処理部
1602
1608
1601
利用条件限定情報作成部
署名検証部
1603
1307
1607
1605
署名鍵記憶部
署名作成部
仲介許諾証作成部
処理制御部
仲介許諾証識別子作成部
仲介許諾証送付作成部
1604
エラーメッセージ作成部
1301
1606
証明証記憶部
入出力制御部
1308
1306
検証用公開鍵DB
仲介許諾証発行履歴DB
1309

【図１７】


スタート
1701
署名の検証に成功したか?
NO
YES
1702
利用許可証仲介許諾証を発行するか?
NO
YES
1703
仲介許諾証識別子の作成
1704
有効期間の決定
1705
利用条件限定情報の決定
1706
仲介許諾証の作成
1707
仲介許諾証送付の作成と出力
1708
仲介許諾証発行履歴の登録
1709
エラーメッセージの作成と出力
終了

【図１８】


1803
仲介許諾証依頼作成部
1810
1804
1801
証明証記憶部
1809
利用許可証依頼処理部
1802
署名鍵記憶部
1807
処理選択部
入出力制御部
仲介許諾証DB
仲介許諾証送付処理部
1805
1806
利用許可証送付処理部
1811
利用許可証仲介プロバイダ用履歴作成部
利用許可証仲介履歴DB
1808
1812
利用許可証仲介依頼者用履歴作成部

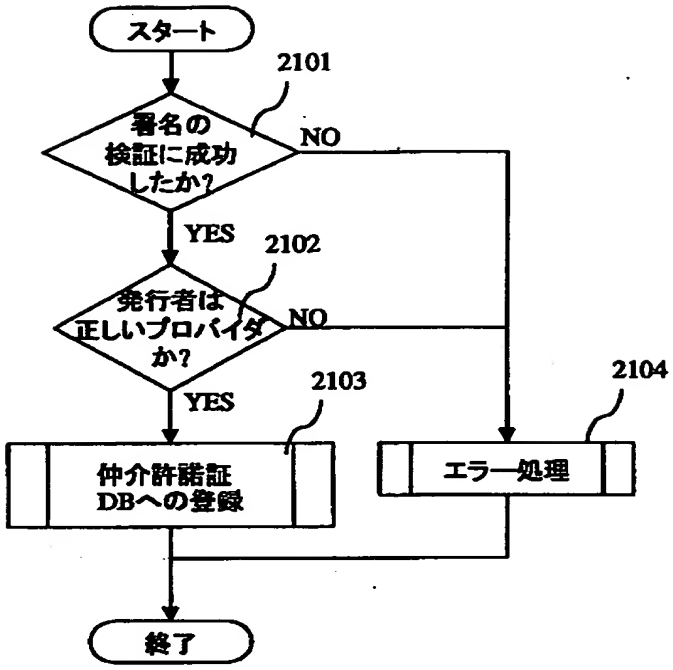
【図１９】

仲介許諾証識別子	公開鍵識別子	プロバイダ識別子	仲介許諾証	プロバイダ証明証
AGM01002	PK00001	PRV10001	FF3AC4...	FE66B...
AGM03010	PK00002	PRV10003	FF3CC2...	FEE4A...
AGM03034	PK00008	PRV10003	FFF87A...	FE7DE...
...	...	...	...	...

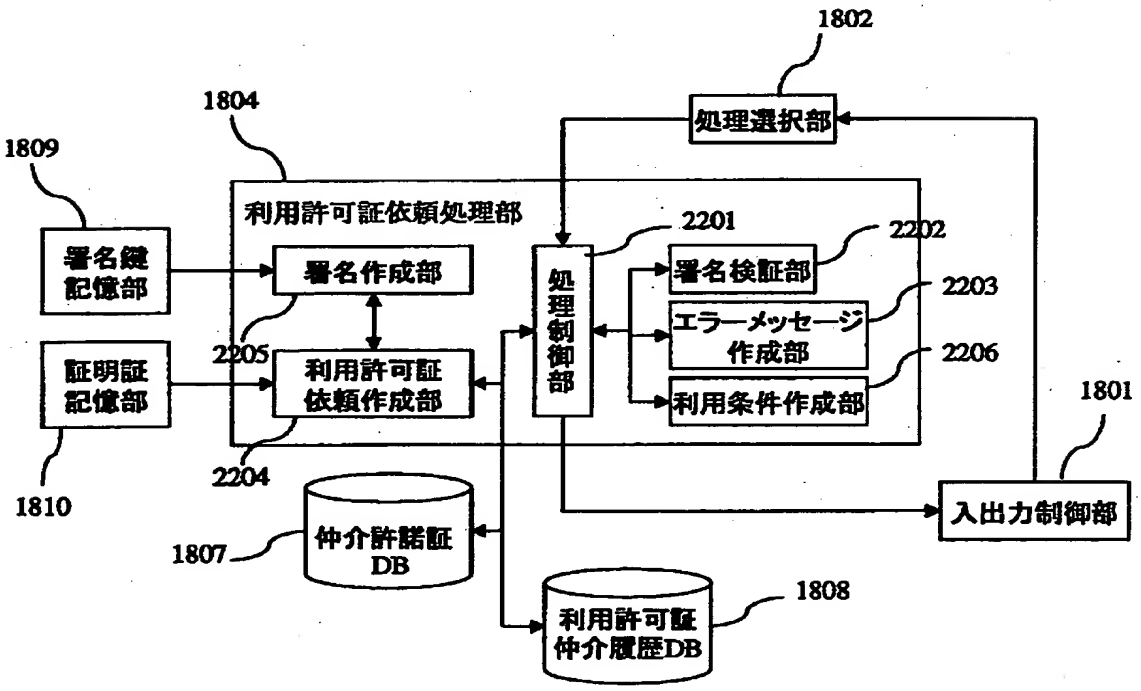
【図２０】

利用許可証識別子	公開鍵識別子	プロバイダ識別子	消費者識別子	依頼者識別子	利用条件	依頼日時	発信日時
TKT10004	PK00001	PRV10001	CNS10006	CNS10006	2F34A...	2000.2.1 10:25	2000.2.1 10:27
TKT10010	PK00008	PRV10003	CNS10003	RTL10024	44FBC...	2000.2.16 18:03	2000.2.16 18:04
	PK00001	PRV10001	CNS10012	CNS10012	5AAB1...	2000.3. 1 03:54	
...	...	...	...		...	...	...

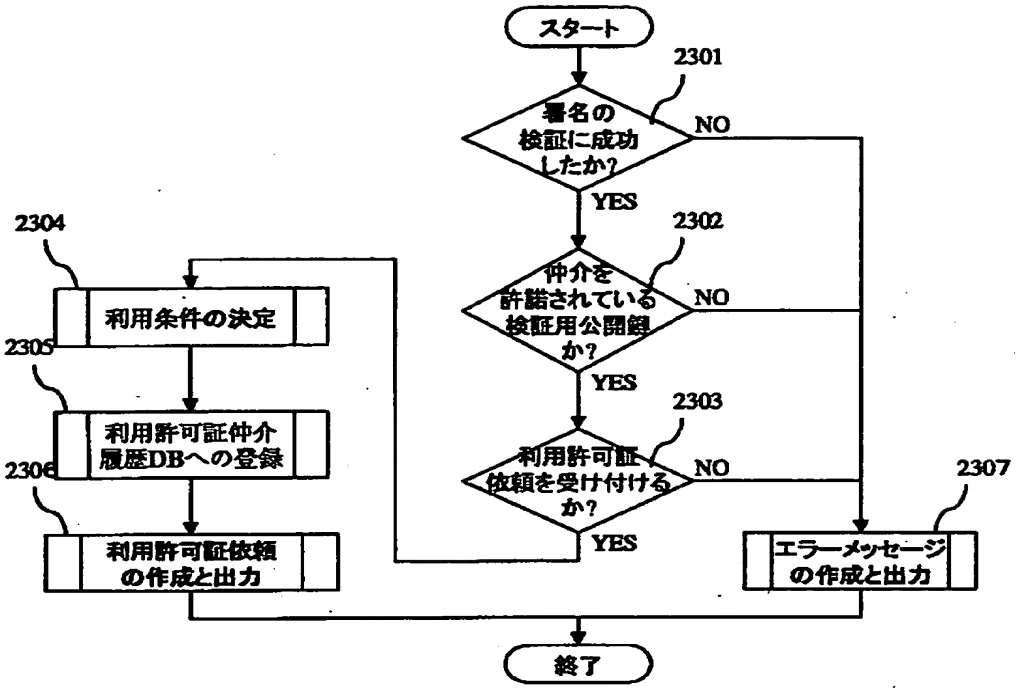
【図２１】


スタート
2101
署名の検証に成功したか?
NO
YES
2102
発行者は正しいプロバイダか?
NO
YES
2103
2104
仲介許諾証DBへの登録
エラー処理
終了

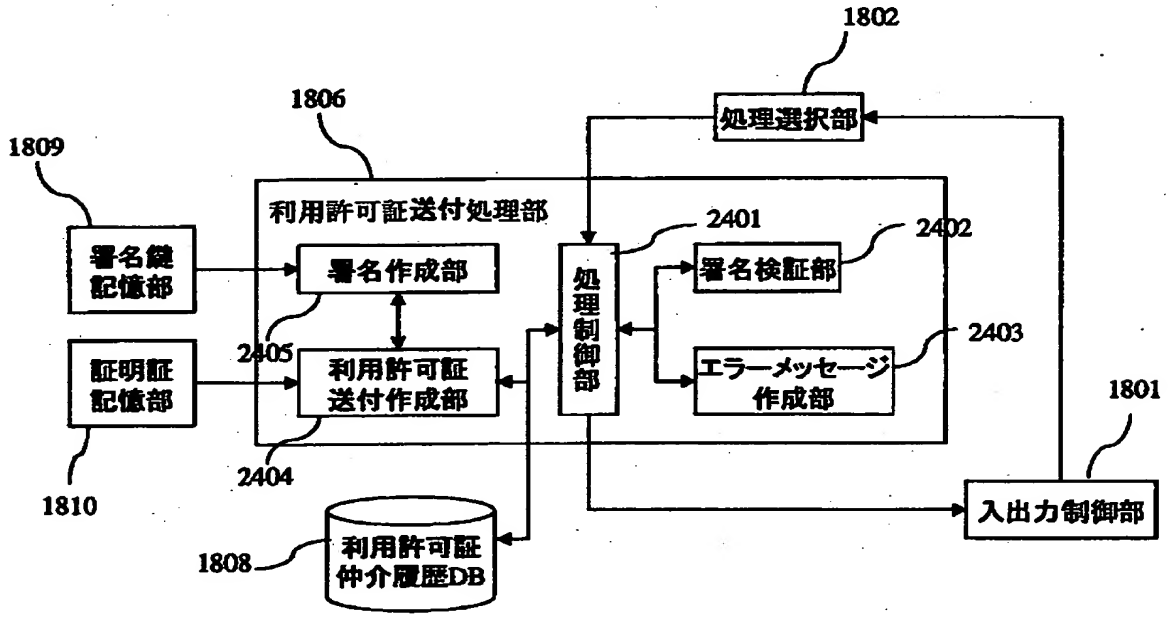
【図２２】


1802
処理選択部
1804
1809
利用許可証依頼処理部
署名鍵記憶部
署名作成部
2201
2202
処理制御部
署名検証部
2203
エラーメッセージ作成部
2205
2206
証明証記憶部
利用許可証依頼作成部
利用条件作成部
1801
2204
1810
入出力制御部
仲介許諾証DB
1807
1808
利用許可証仲介履歴DB

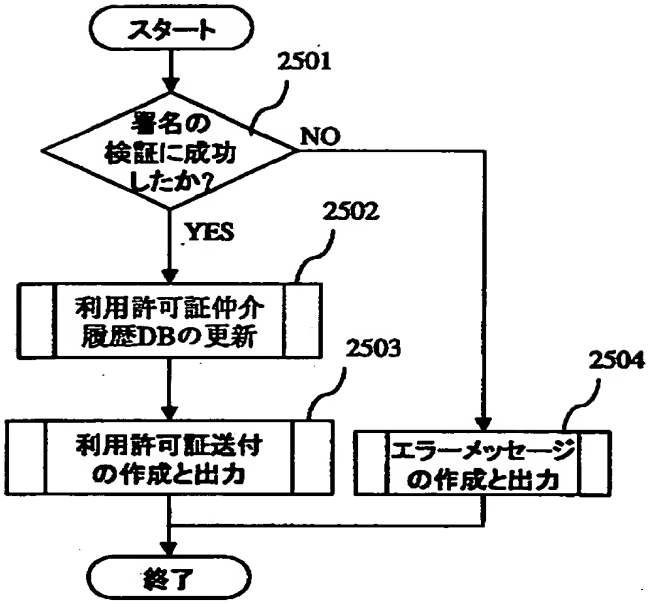
【図２３】


スタート
2301
署名の検証に成功したか?
NO
YES
2302
仲介を許諾されている検証用公開鍵か?
NO
YES
2303
利用許可証依頼を受け付けるか?
NO
YES
2304
利用条件の決定
2305
利用許可証仲介履歴DBへの登録
2306
利用許可証依頼の作成と出力
2307
エラーメッセージの作成と出力
終了

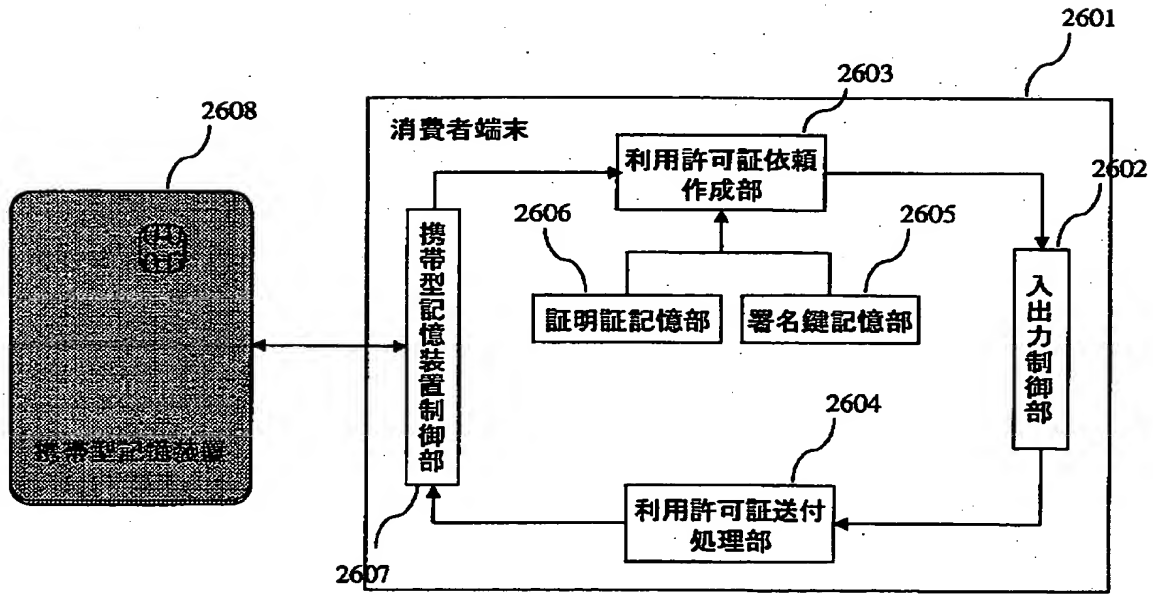
【図２４】


1802
処理選択部
1806
利用許可証送付処理部
1809
署名鍵記憶部
署名作成部
2401
処理制御部
2402
署名検証部
2405
証明証記憶部
利用許可証送付作成部
2403
エラーメッセージ作成部
1801
2404
1810
入出力制御部
1808
利用許可証仲介履歴DB

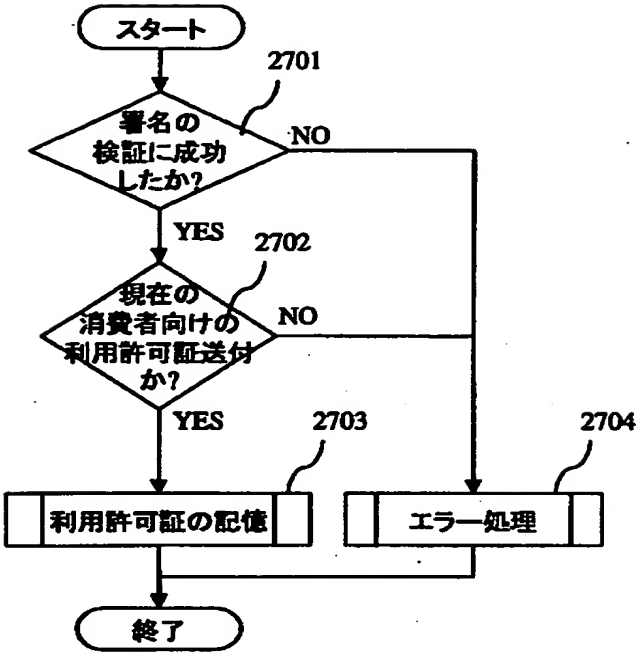
【図２５】


スタート
2501
署名の検証に成功したか?
NO
YES
2502
利用許可証仲介履歴DBの更新
2503
利用許可証送付の作成と出力
2504
エラーメッセージの作成と出力
終了

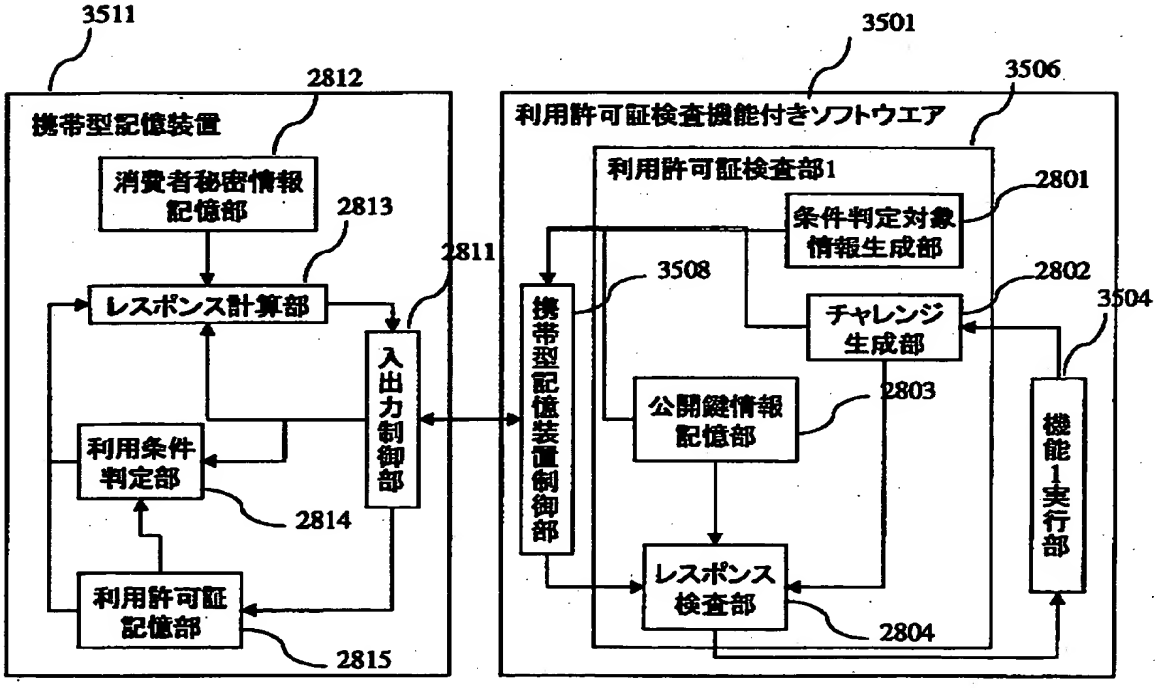
【図２６】


2601
2603
2608
消費者端末
利用許可証依頼作成部
2602
2606
2605
携帯型記憶装置制御部
証明証記憶部
署名鍵記憶部
入出力制御部
2604
利用許可証送付処理部
2607

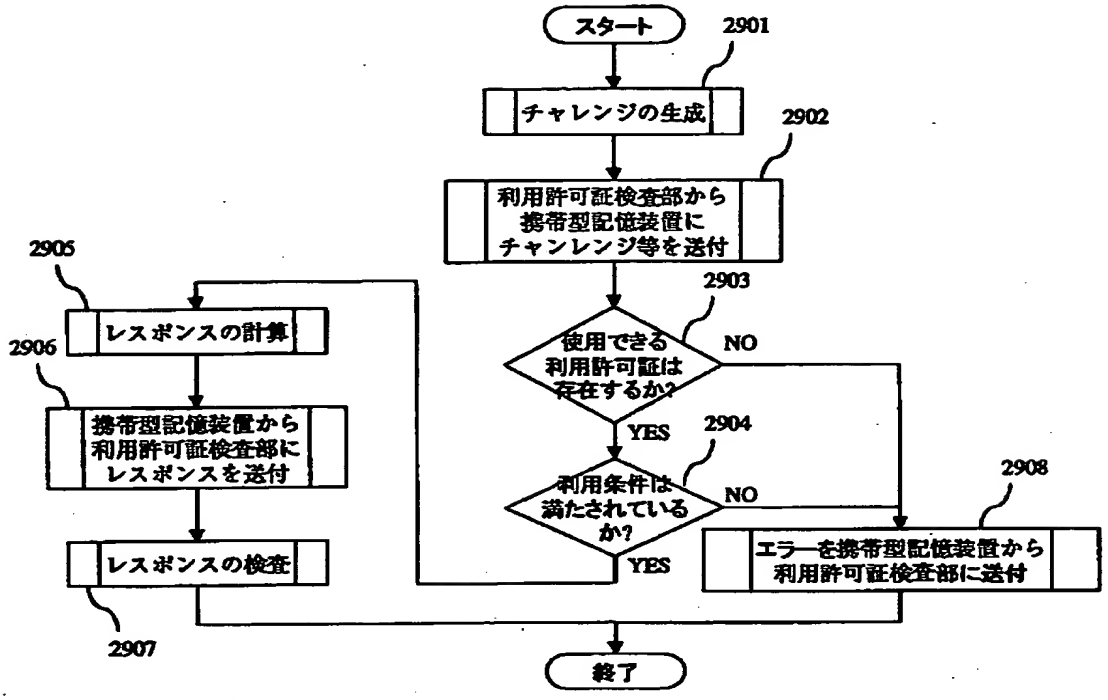
【図２７】


スタート
2701
署名の検証に成功したか?
NO
YES
2702
現在の消費者向けの利用許可証送付か?
NO
YES
2703
2704
利用許可証の記憶
エラー処理
終了

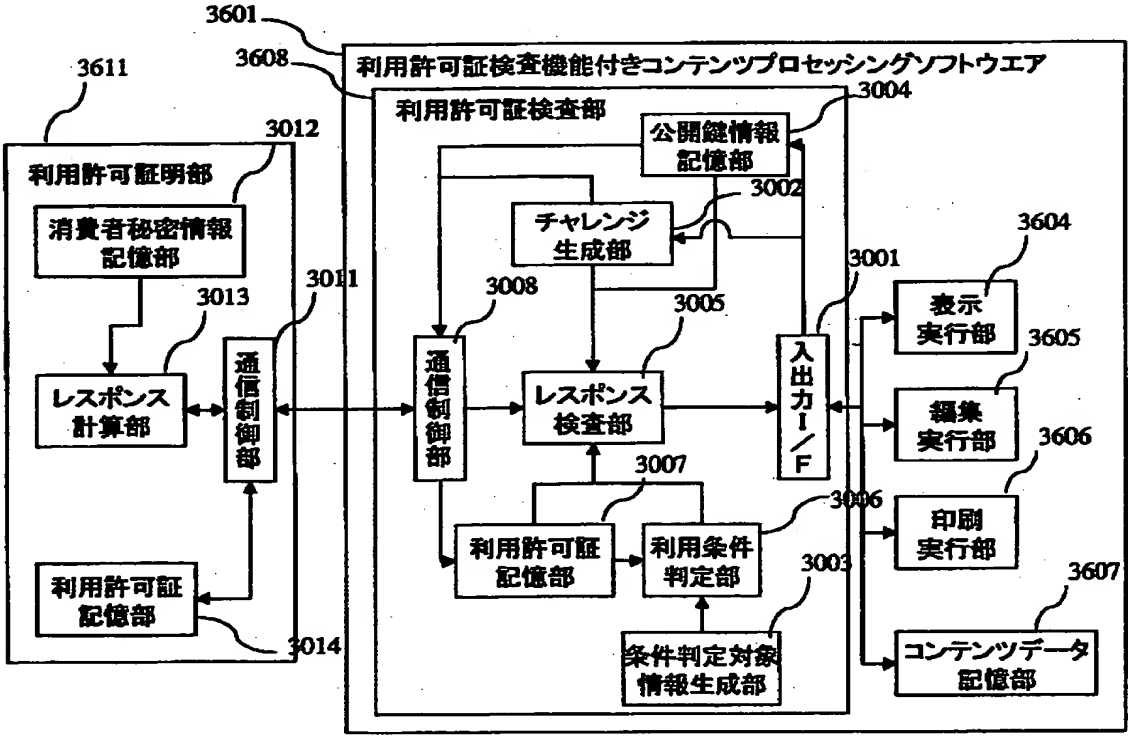
【図２８】


3511
2812
携帯型記憶装置
消費者秘密情報記憶部
2813
レスポンス計算部
2811
入出力制御部
利用条件判定部
2814
利用許可証記憶部
2815
3501
3506
利用許可証検査機能付きソフトウエア
利用許可証検査部1
2801
条件判定対象情報生成部
3508
携帯型記憶装置制御部
2802
チャレンジ生成部
3504
公開鍵情報記憶部
2803
機能1実行部
レスポンス検査部
2804

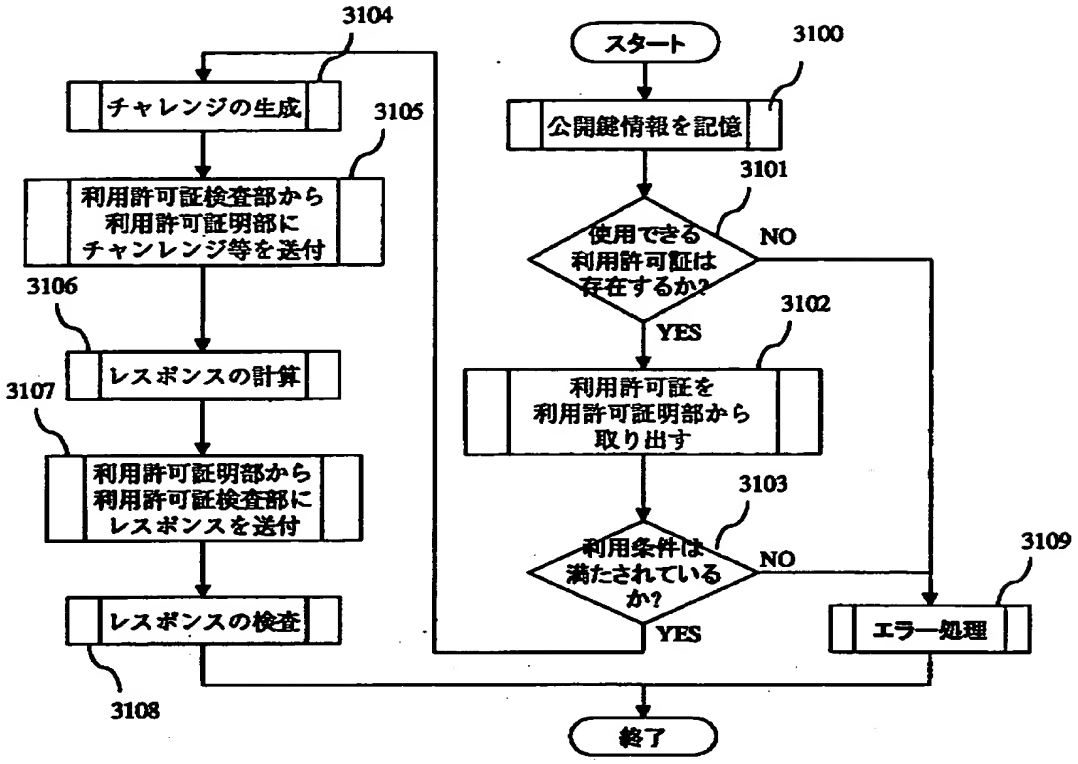
【図２９】


スタート
2901
チャレンジの生成
2902
利用許可証検査部から携帯型記憶装置にチャレンジ等を送付
2903
使用できる利用許可証は存在するか?
NO
YES
2904
利用条件は満たされているか?
NO
YES
2905
レスポンスの計算
2906
携帯型記憶装置から利用許可証検査部にレスポンスを送付
レスポンスの検査
2907
2908
エラーを携帯型記憶装置から利用許可証検査部に送付
終了

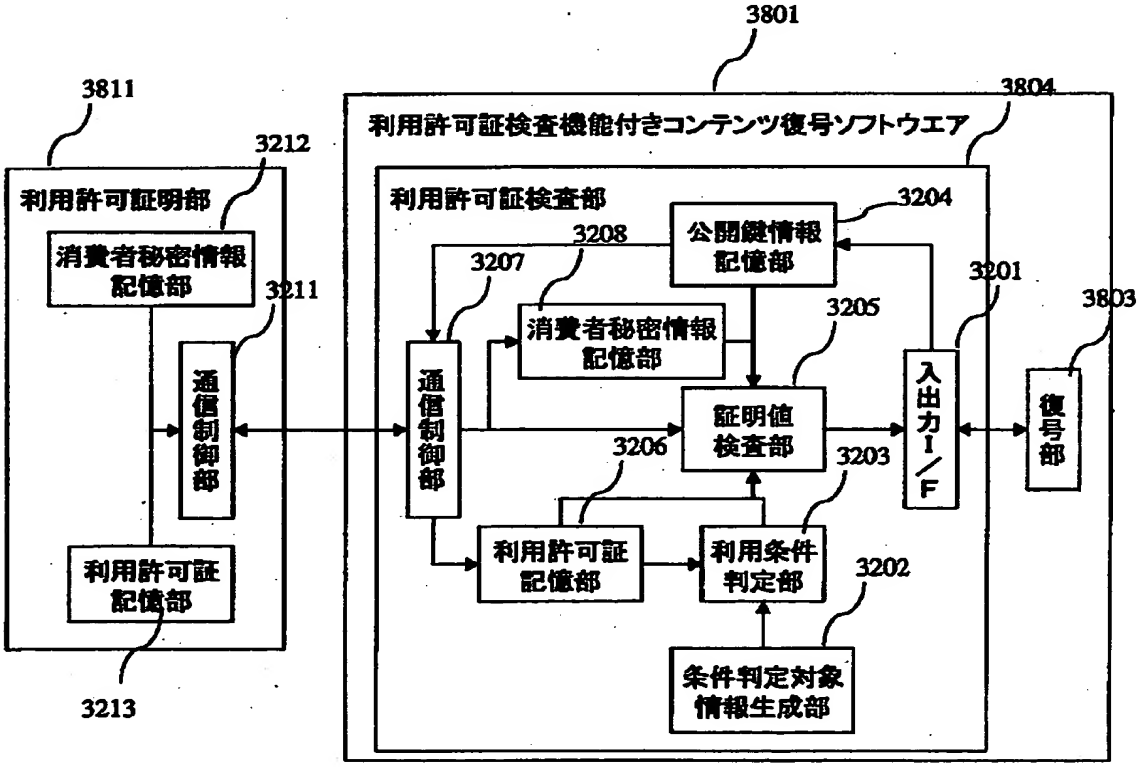
【図３０】


3601
利用許可証検査機能付きコンテンツプロセッシングソフトウエア
3608
利用許可証検査部
3004
公開鍵情報記憶部
3002
チャレンジ生成部
3005
レスポンス検査部
3007
利用許可証記憶部
3006
利用条件判定部
3003
条件判定対象情報生成部
3008
通信制御部
3001
入出力I／F
3611
利用許可証明部
3012
消費者秘密情報記憶部
3013
レスポンス計算部
3011
通信制御部
3014
利用許可証記憶部
3604
表示実行部
3605
編集実行部
3606
印刷実行部
3607
コンテンツデータ記憶部

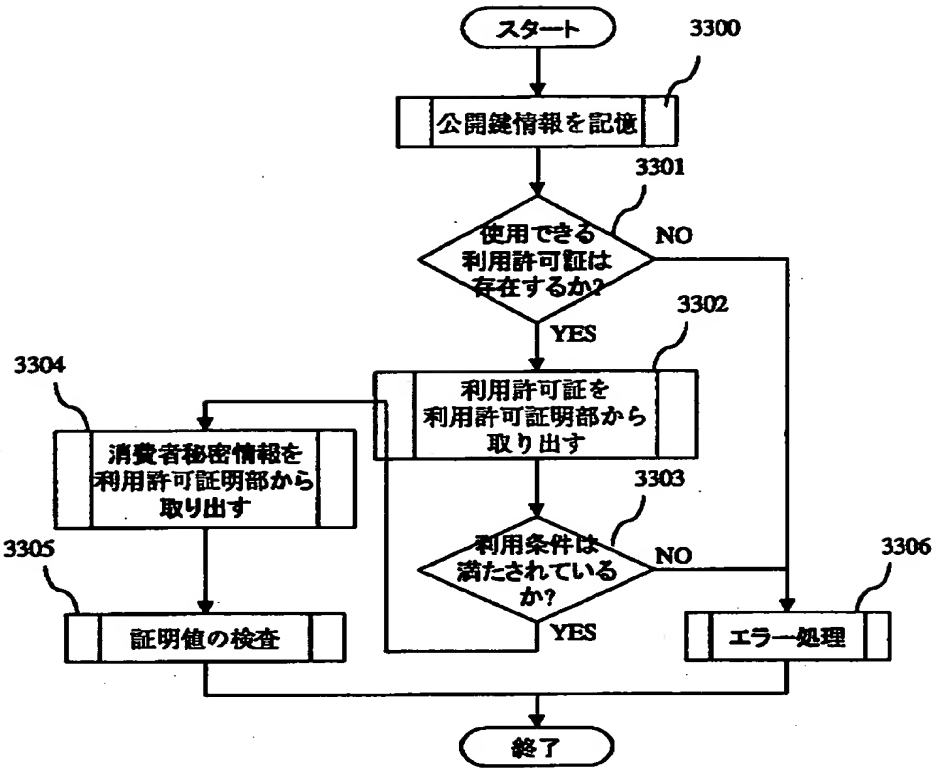
【図３１】


スタート
3100
公開鍵情報を記憶
3101
使用できる利用許可証は存在するか?
NO
YES
3102
利用許可証を利用許可証明部から取り出す
3103
利用条件は満たされているか?
NO
YES
3104
チャレンジの生成
3105
利用許可証検査部から利用許可証明部にチャンレンジ等を送付
3106
レスポンスの計算
3107
利用許可証明部から利用許可証検査部にレスポンスを送付
レスポンスの検査
3108
エラー処理
3109
終了

【図３２】


3801
利用許可証検査機能付きコンテンツ復号ソフトウエア
3804
3811
利用許可証明部
3212
消費者秘密情報記憶部
3211
通信制御部
利用許可証記憶部
3213
利用許可証検査部
3204
公開鍵情報記憶部
3208
3207
消費者秘密情報記憶部
3205
通信制御部
証明値検査部
3206
3203
利用許可証記憶部
利用条件判定部
3202
条件判定対象情報生成部
3201
入出力I/F
3803
復号部

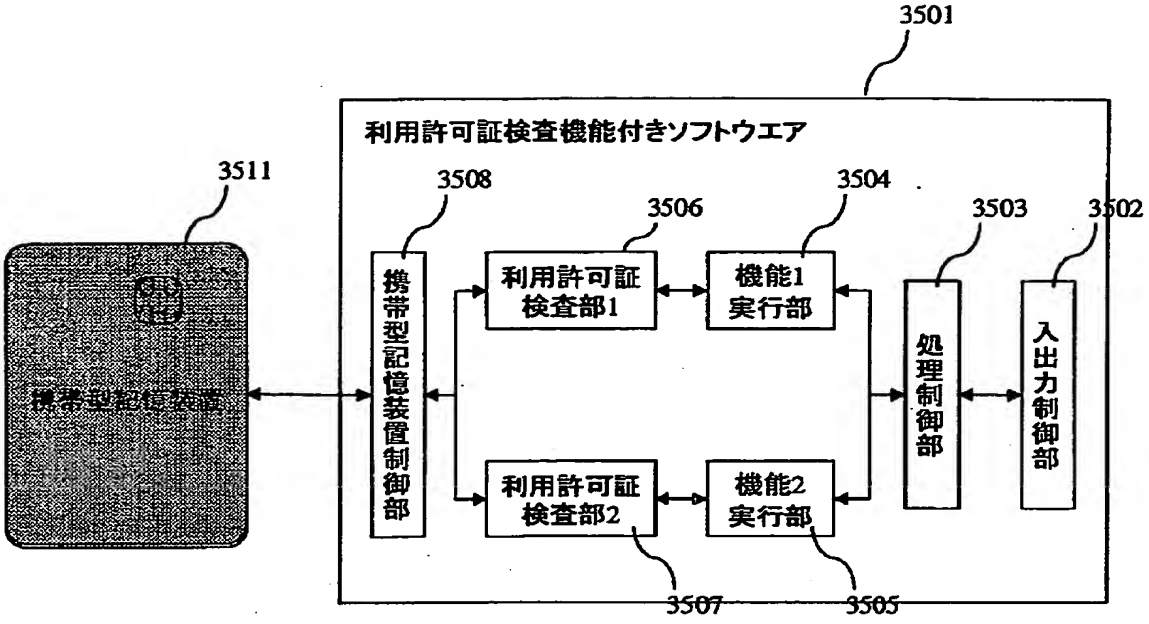
【図３３】



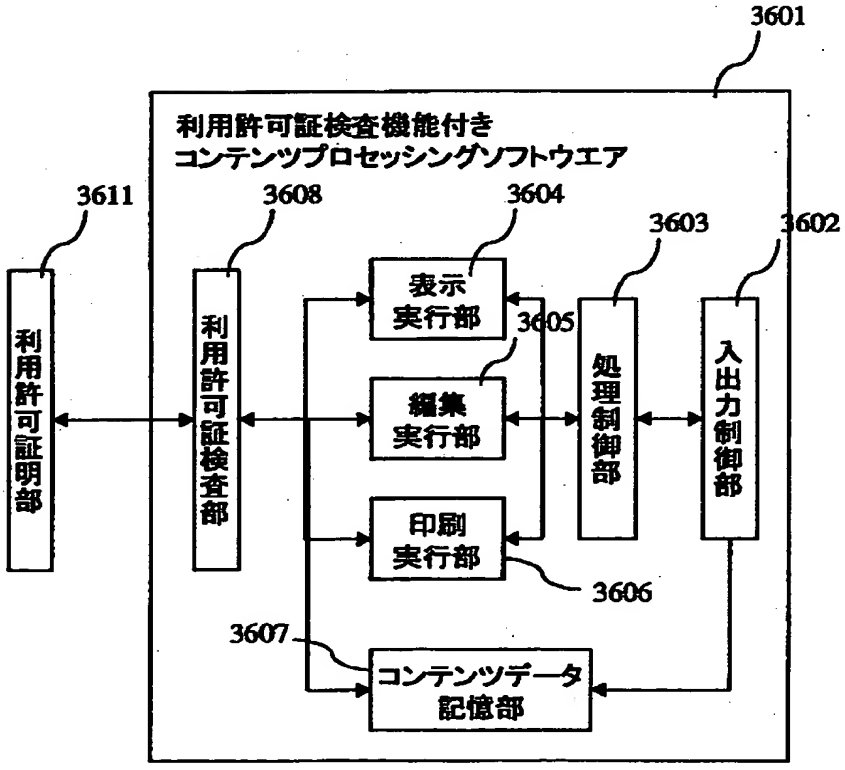
【図３４】

利用許可証仲介許諾証識別子	公開鍵識別子	リテーラ識別子	利用条件限定情報	有効期間開始	有効期間終了	発行日
AGM01002	PK00001	RTL10001	FF3AC4...	1999.12.1	2000.11.31	1999.12.1
AGM03010	PK00002	RTL10003	FF3CC2...	2000.1.1	2000.7.1	2000.1.1
AGM03034	PK00008	RTL10003	FFF87A...	2000.3.4	2001.3.4	2000..3.3
...	...	...	...	...	...	...

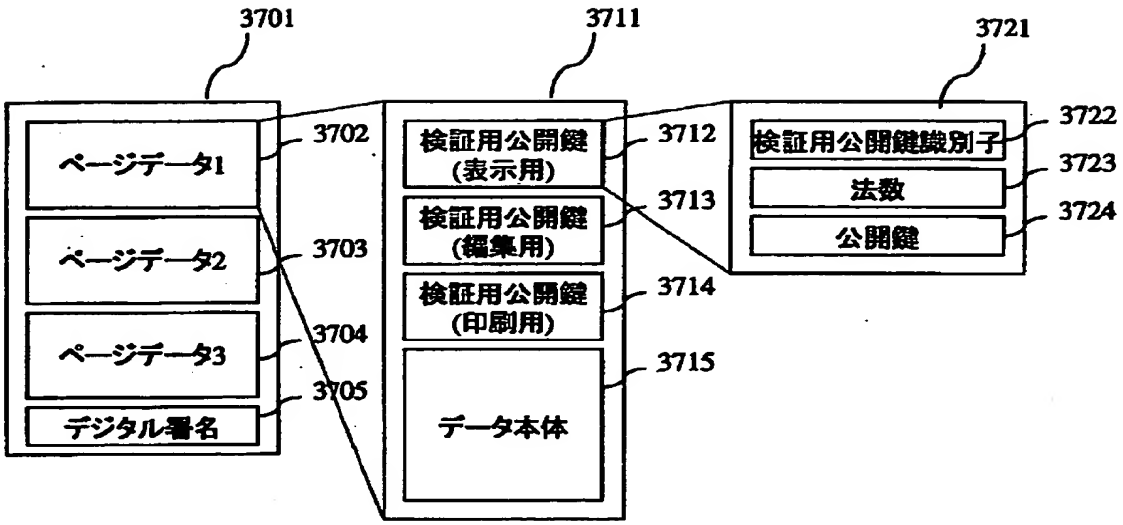
【図３５】


3501
利用許可証検査機能付きソフトウエア
3511
3508
3506
3504
3503
3502
携帯型記憶装置
携帯型記憶装置制御部
利用許可証検査部1
機能1実行部
処理制御部
入出力制御部
利用許可証検査部2
機能2実行部
3507
3505

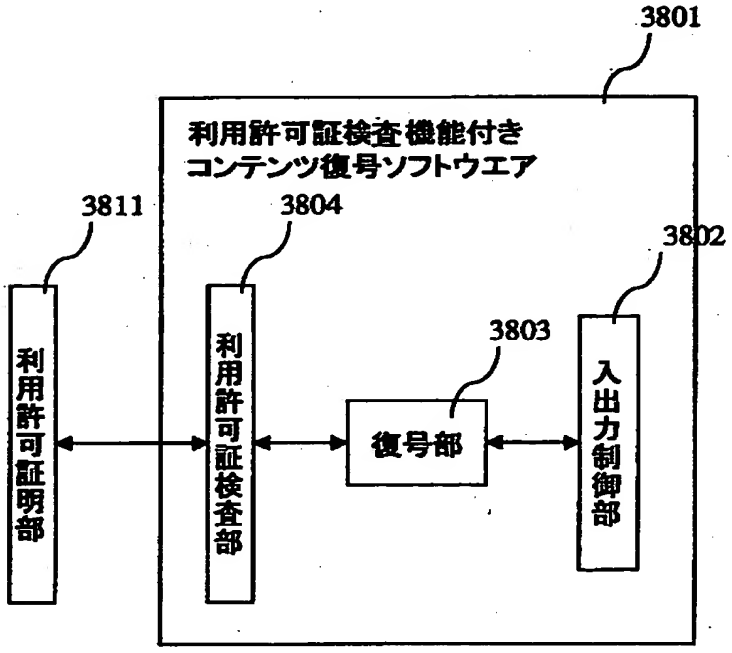
【図３６】


3601
利用許可証検査機能付き
コンテンツプロセッシングソフトウエア
3611
3608
3604
3603
3602
利用許可証明部
利用許可証検査部
表示実行部
3605
編集実行部
処理制御部
入出力制御部
印刷実行部
3606
3607
コンテンツデータ記憶部

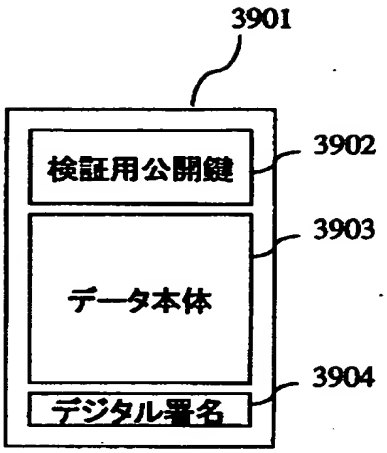
【図３７】


3701
3711
3721
ページデータ1
ページデータ2
ページデータ3
デジタル署名
3702
3703
3704
3705
検証用公開鍵
(表示用)
検証用公開鍵
(編集用)
検証用公開鍵
(印刷用)
データ本体
3712
3713
3714
3715
検証用公開鍵識別子
法数
公開鍵
3722
3723
3724

【図３８】


3801
利用許可証検査機能付き
コンテンツ復号ソフトウエア
3811
3804
3802
3803
利用許可証明部
利用許可証検査部
復号部
入出力制御部

【図３９】



【書類名】　要約書

【要約】

【課題】　デジタルコンテンツ提供者、販売者が自らのリソースを消費することなく利用許可証を消費者に発行できるようにする。

【解決手段】　リテーラ１０３は消費者端末１０９にインターネット１０１を介してデジタルコンテンツを販売する。リテーラ１０３はデジタルコンテンツおよび購入者に応じた利用許可証の発行を利用許可証発行センタ１０２に要求して利用許可証を受領する。消費者端末１０９はリテーラ１０３からインターネット１０１を介して利用許可証を受け取る。消費者はプロバイダ１０５から提供を受けたデジタルコンテンツを利用する際に、利用許可証を用いて正規の購入者であることを証明する。証明が成功裏に検証されたときに、消費者はデジタルコンテンツを利用できるようになる。

【選択図】　図１

出　願　人　履　歴　情　報

識別番号　　〔０００００５４９６〕

１．変更年月日　　１９９６年　５月２９日
［変更理由］　住所変更
住　所　　東京都港区赤坂二丁目１７番２２号
氏　名　　富士ゼロックス株式会社